T E C H N I C K Á U N I V E R Z I T A V L I B E R C I

Fakulta mechatroniky, informatiky a mezioborových studií

D I P L O M O V Á P R Á C E

2009 Bc. Jan Laurin

Technická univerzita v Liberci
Fakulta mechatroniky, informatiky a mezioborových studií

Studijní program: **N 2612 – Elektrotechnika a informatika**
Studijní obor: **Informační technologie**

Možnosti využití čipových karet v městských aglomeracích

Possible usage of Smart Cards in Urban Agglomerations

Bc. Jan Laurin

Vedoucí práce: Doc. Ing. Jan Skrbek, Dr., katedra informatiky
Konzultant: Ing. Jiří Hruboň, Liberecká IS, a. s.

Počet stran: 81

Datum odevzdání: 29. května 2009

Prohlášení

Byl jsem seznámen s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé diplomové práce pro vnitřní potřebu TUL.

Užiji-li diplomovou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Diplomovou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím diplomové práce a konzultantem.

V Liberci dne 29. května 2009 Bc. Jan Laurin

Abstrakt

Diplomová práce na téma „Možnosti využití čipových karet v městských aglomeracích“ se zaměřuje na využití elektronických identifikačních systémů v oblasti podpory turismu v regionu. Většina velkých měst systém čipové karty využívá, ale z velké části jen pro městskou hromadnou dopravu. Městské karty jsou většinou určeny pro obyvatele daného města. Zavedením turistické čipové karty se nabízené funkce jednoúčelové karty rozšíří a nabídnou uživatelům větší komfort. Na rozdíl od městské karty by měla být turistická karta určena především pro návštěvníky regionu. Měla by poskytnout výhody, jako jsou elektronická peněženka, platba za MHD, lanovky, vleky, hotely, parkovné, služby cestovního ruchu – koncerty, aquaparky a různé slevové systémy. Turistická karta by měla propojit několik systémů, které již v regionu fungují. Diplomová práce je studií proveditelnosti zavedení turistické čipové karty v Libereckém regionu, která obsahuje možnosti a způsoby využití čipových karet, zmiňuje používaná zařízení pro komunikace karty s okolím a jejich funkce, bezpečnost čipových karet a ochranu osobních údajů, návrh architektury a popis procesů zavedení čipové karty. V závěru práce jsou zhodnocena východiska používání čipových karet v městských aglomeracích.

Klíčová slova

Čipové karty, identifikace, městské aplikace, městské karty

Abstract

The subject of this thesis is Possible usage of Smart Cards in Urban Agglomerations. It is focused on a usage of electronic identification systems within the field of promotion the turism in the region. Most of large cities are already using the smart card system, but in most cases for public transport only. City Cards are mainly intended for residents of given cities. Implementation of a turist smart card gives the users more functions to use as well as better comfort. Intention of the turist card, unlike the city card, is to be used by visitors of the region. It should provide such benefits like an electronic wallet, possible payment for public transport, cablecars, ski-lifts, hotel, parking, tourist services: concerts, aquaparks and various discount systems. Tourist card should connect several systems already operating in the region. This thesi is a feasibility study of tourist smart card implementation within the Liberec region. It includes options and ways of using smart cards, mentions the equipment used for communication of the card with its surroundings and its functions, security of smart cards and personal data protection, an architecture concept and description of processes for smart card implementation. The conclusion of this thesis evaluates data related to usage of smart cards in urban agglomeration.

Key Words

City cards, identification, smart cards, urban applications

Obsah

Seznam zkratek **8**
Seznam tabulek **11**
Seznam obrázků **12**
Úvod **13**
1. Možnosti a způsoby použití čipových karet **16**
1.1 Historie elektronických karet 16
1.2 Přehled identifikačních prvků 17
1.3 Využití čipových karet v jednotlivých oblastech 22
Odbavovací systémy 23
Elektronická peněženka 23
Rezervační systém 23
Stravovací systém 24
Přístupový systém 24
Slevové a věrnostní programy 24
1.4 Specifikace služeb a požadavků na turistickou kartu 25
1.5 Standardizace a normalizace v oblasti čipových karet 26
1.6 Technologie MIFARE 29
2. Používaná zařízení a jejich funkce pro práci s daty a komunikaci karty s okolím **36**
2.1 Bankomaty, terminály 36
2.2 Mobilní automaty pro městskou dopravu 37
3. Ochrana osobních údajů držitelů karet a související legislativa **42**
3.1 Návrh zpracování osobních údajů u turistické karty 42
3.2 Legislativa související s ochranou osobních údajů 43
4. Bezpečnost bezkontaktních čipových karet **45**
4.1 Obecné ochranné prvky 45
4.2 Elektronické bezpečnostní prvky turistické karty 47
4.3 Kombinace ochranných prvků 48
4.4 Možnosti zneužití čipové karty 49
4.5 Standardy bezpečnosti čipových karet 49
5. Návrh architekury systému a popis procesů **53**

5.1 Celková architektura 53
5.2 Aplikační software 61
5.3 Struktura kódu 63
5.4 Komponenty systému – nároky na vybavení 63
5.5 Kartové centrum 67

6. Zhodnocení východisek používání čipových karet v městských aglomeracích 68
6.1 Shrnutí vlastností technologií dle typu média 68
6.2 Rozpočet 71
6.3 Časový harmonogram 72
6.4 Výhled do budoucnosti 74

7. Závěr 75
Seznam použité literatury 77

Seznam zkratek

AES	Symetrická bloková šifra *(Advanced Encryption Standard)*
AID	Identifikátor aplikace *(Application Identifier)*
API	Rozhraní pro programování aplikací *(Application Programming Interface)*
ATM	Bankomat *(Automatic Teller Machine)*
CAN	Sběrnice pro vnitřní komunikační síť senzorů *(Controller Area Network)*
cca	Přibližně *(cirka)*
CICC	Technologie bezkontaktních čipových karet *(Close Coupled Cards)*
CRC	Cyklický redundantní součet *(Cyclic Redundancy Check)*
ČSN	Česká soustava norem, Česká technická norma
DES	Symetrický šifrovací algoritmus *(Data Encryption Standard)*
EEPROM	Přepisovatelná paměť *(Electrically Erasable Programmable Read-Only Memory*)
EMV	Globální standard pro vzájemné fungování integrovaných obvodů karet *(Europay, MasterCard, VISA)*
GB	Gigabyte *(jednotka množství dat)*
GbE	Gigabit Ethernet
GHz	Gigahertz *(jednotka frekvence)*
GPS	Globální družicový polohový systém *(Global Positioning Systém)*
HW	Hardware
IEC	Standardizační organizace pro všechny oblasti elektrotechniky *(International Electrotechnical Commision)*
ID	Jednoznačný identifikátor
IrDa	Infračervený port *(Infrared Data Association)*
ISO	Mezinárodní organizace pro standardizaci (*International Organization for Standardization)*

LED	Dioda emitující světlo *(Light-Emitting Diode)*
MAC	Autentizační kód zprávy *(Message Authentication Code)*
MB	Megabyte *(jednotka množství dat)*
Mb/s	Megabit za sekundu *(přenosová rychlost)*
MHD	Městská hromadná doprava
NFC	Bezdrátová technologie pro přenos dat na krátkou vzdálenost (*Near Field Communication)*
OS	Operační systém
OS SCFW	Operační systém čipových karet pro Windows *(Operating System Smart Card for Windows)*
PDA	Kapesní počítač *(Personal Digital Assistant)*
PHP	Skriptovací programovací jazyk *(Personal Home Page)*
PICC	Technologie bezkontaktních čipových karet *(Proximity Range Cards)*
PIN	Osobní identifikační kód *(Personal Identification Number)*
PKI	Infrastruktura veřejného klíče *(Public Key Infrastructure)*
POS	Platební terminály prodejců *(Point of Sale)*
RAID	Metoda zabezpečení dat proti selhání pevného disku (*Redundant Array of Inexpensive/Independent Discs)*
RAM	Paměť s přímým přístupem *(Random Access Memory)*
RFID	Identifikace na rádiové frekvenci *(Radio Frequency Identification)*
SAM	Bezpečnostní modul pro vstup *(Security Access Module*)
SEO	Optimalizace pro vyhledávače *(Search Engine Optimization)*
SIM karta	Účastnická identifikační karta v mobilní síti (S*ubscriber Identity Module)*
SSL	Protokol, vrstva vložená mezi vrstvu transportní a aplikační *(Secure Sockets Layer)*
SQL	Strukturovaný dotazovací jazyk (*Structured Query Language)*
SW	Software

UPS	Systém zajišťující souvislou dodávku elektřiny *(Uninterruptible Power Supply /Source)*
USA	Spojené státy americké *(United States of America)*
USB	Univerzální sériová sběrnice *(Universal Serial Bus)*
VICC	Technologie bezkontaktních čipových karet *(Vicinity Range Cards)*
WORM	Jednorázově zapisovatelná paměť *(Write Once Read Many Times)*

Seznam tabulek

Tabulka 1: Tabulka s technickými parametry NFC, RFID, IrDa a Bluetooth 21
Tabulka 2: Popis požadovaných služeb a jednotlivých technologií 25
Tabulka 3: Technické parametry technologie MIFARE 31
Tabulka 4: Formáty karet 50
Tabulka 5: Konceptuální návrh struktury databáze evidenčního listu 58
Tabulka 6: Koncepce návrhu struktury dat evidenčního typu karty 60
Tabulka 7: Shrnutí vlastností technologií dle typu média 69
Tabulka 8: Rozpočet 71
Tabulka 9: Časový harmonogram 73

Seznam obrázků

Obrázek 1: Čipová karta.....18
Obrázek 2: Bezkontaktní čipová karta.....19
Obrázek 4: Duální čipová karta.....20
Obrázek 3: Hybridní čipová karta.....20
Obrázek 5: Schéma norem kontaktních a bezkontaktních čipových karet.....28
Obrázek 6: Schéma norem bezkontaktních čipových karet.....29
Obrázek 7: Čtečka čipových karet – CKC.....37
Obrázek 8: Mobilní automat na výdej jízdenek - AVJ F.....38
Obrázek 9: Terminál pro bezkontaktní karty.....40
Obrázek 10: Terminál pro bezkontaktní karty.....41
Obrázek 12: Architektura systému.....53

Úvod

Čipové karty se staly fenoménem začátku 21. století jako médium aplikované při identifikaci či autentizaci osob nebo jako médium pro bezhotovostní platební transakce za úhradu služeb.[1] Důvodem jejich masivního rozvoje byla snaha nabídnout občanům měst jednotné identifikační, autorizační a platební médium pro čerpání služeb poskytovaných jak veřejnou správou, tak i komerčními subjekty, kteřé v daném regionu působí. Dalším důvodem byla ekonomická výhodnost pro nejen pro uživatele ale také pro provozovatele karetních systémů.

Městské karty se postupně od svého nasazení staly standardem větších měst. V poslední době se využívají stále častěji i pro specifická okrajová řešení v různých odvětvích. Ucelená technická řešení tak pokrývají požadavky určitých cílových skupin v uzavřených geografických oblastech. Hlavním cílem diplomové práce je vypracování podkladů pro přípravu projektové dokumentace zavedení turistické čipové karty. V dílčích cílech jsou poté popsány technologické možnosti identifikačních médií, analýza legislativního prostředí této oblasti, ochrana osobních údajů uživatelů a rozbor používaných zabezpečení.

Turistická karta rozšiřuje stávající funkce standardní městské karty, která ve většině měst slouží zejména pro služby městské hromadné dopravy. Navrhované řešení by mělo být multifunkční slevovou kartou, která držitelům umožní volné nebo zlevněné vstupy do vybraných turistických atraktivit a čerpání slev na různé další služby. Karta obsahuje funkci elektronické peněženky, kterou bude možné uhradit poplatek za městskou hromadnou dopravu, vleky, lanovky, vstupy do kulturních a turistických zařízení (muzeum, zoo,….), parkovné apod. Turistická karta Liberecka je produkt, jehož cílem je podpořit regionální turistický ruch. Karta je určena pro turisty, zahraniční i domácí, obyvatele Libereckého kraje a přilehlých regionů i pro cestovní kanceláře. Turistická karta by navíc měla sloužit jako nástroj ke zvýšení informovanosti zmíněných návštěvníků kraje o jeho atraktivitách. Formou volných vstupů a slev motivuje turisty k jejich návštěvě a navíc nabízí také slevy na další služby (sportovní aktivity, restaurace, lázně apod).

[1] HENDRY, M. *Smart Card Security and Applications.* Boston, 2001

Diplomová práce vychází z dříve realizovaných funkčních rešení, přičemž navrhuje kvalitativně nové postupy a využití. Zavedení turistických městských karet by však vyžadovalo provedení podrobné studie proveditelnosti a finanční analýzy prostředí. Na základě těchto rozborů by bylo možné stanovit optimální technické řešení a nastavení postupů pro implementaci. První kapitola obsahuje stručnou historii čipových karet, porovnává jednotlivé technologie, jako jsou čárový kód, čip, NFC. Úvodní kapitola také popisuje využití čipových karet v jednotlivých oblastech – odbavovací systémy, stravovací systémy, elektronická peněženka. V kapitole jsou popsány požadavky na turistickou čipovou kartu, to znamená funkce, které by měla turistická karta Liberecka splňovat. Závěr první kapitoly se věnuje standardizaci čipových karet (normy ISO) a výběr druhu čipové karty vhodné pro funkce turistické čipové karty (technologie MIFARE).

Druhá kapitola obsahuje popis používaných zařízení a jejich funkce pro práci s daty a komunikaci karty s okolím. Popisuje speciální bankomaty pro dobití elektronické peněženky na kartě a čtečky čipových karet. Kapitola se věnuje také popisu automatů pro městskou hromadnou dopravu.

Třetí kapitola se týká ochrany osobních údajů držitelů karet a související legislativy. Kapitola obsahuje návrh, jak data získaná od uživatelů zpracovávat. Popisuje části zákonů a vyhlášek souvisejících s ochranou osobních údajů.

Další kapitola shrnuje obecné bezpečnostní prvky, neelektronické, jako jsou barva karty, fotografie na kartě apod. Dále jsou zde popsány elektronické bezpečnostní prvky, které zajišťují bezpečnost bezkontaktních čipových karet (segmenty vhodné pro turistickou kartu i prvky, které turistická karta nevyžaduje). Jsou zde popsány také možnosti zneužití čipové karty a standardy, jež jsou vázány na bezpečnost čipových karet.

V páté kapitole je popsán návrh architektury systému a systémových procesů turistické karty. Jsou zde podrobně rozepsány celková architektura a funkcionality systému. Podkapitola aplikační software obsahuje popis řídící aplikace systému a aplikace pro terminály čipové karty. V kapitole je stručně popsána struktura kódu obsaženého na čipové kartě. Podkapitola komponenty systému (nároky na vybavení) zmiňuje konkrétní zařízení potřebné pro funkčnost celého systému. Poslední část této kapitoly přibližujefunkci kartové centruma, které bude celý systém turistické karty řídit.

Poslední šestá kapitola hodnotí východiseka používání čipových karet v městských aglomeracích. Porovnáná vlastností technologií dle typu média, ze kterého by čipová karta měla vycházet. Kapitola obsahuje odhad nákladů zavedení turistické karty v regionu a časový harmonogram celé implementace systému. Poslední částí kapitoly je výhled do budoucnosti, kde jsou uvedeny technologie, které brzy čipovou kartu v určitých oblastech nahradí.

1. Možnosti a způsoby použití čipových karet

První kapitola obsahuje stručný popis historie elektronických karet. Následuje přehled identifikačních prvků, jako je čárový kód, magnetický záznam, čipová karta apod. V první kapitole je obsažen stručný popis využití čipových karet v jednotlivých oblastech (doprava, finanční oblast, …). Dále je v první kapitole popsána standardizace a normalizace v oblasti čipových karet, jsou zde popsány normy ISO, které musí být při zavádění karet do provozu splněny. Kapitola obsahuje také výběr vhodného média pro navrhovaný systém a jeho popis (čipová karta). Poslední část první kapitoly popisuje technologii MIFARE, její typy a specifické vlastnosti této technologie.

Diplomová práce se zaměřuje na turistickou kartu. Turistická karta je identifikační médium, které spojuje čerpané služby se zákazníkem (jednotlivcem, rodinou, či jinými skupinami). Služby, které jsou poskytovány prostřednictvím turistické karty, jsou například jízdné MHD, elektronická peněženka, vstupy do rozličných areálů a sportovišť, slevové poukazy apod. Možnou variantou pro turistickou kartu by mohl být čárový kód vytištěný na papíru nebo plastové kartě, ten ovšem zdaleka nepojme takové množství dat jako čipová karta, na druhou stranu, je to jedna z levnějších variant. Další možnou technologií by byla technologie NFC, která je nejčastěji uzpůsobena pro chytré mobilní telefony. Pořizovací cena chytrého telefonu pro jedince je mnohonásobně vyšší než zakoupení čipové karty. Z výše uvedených informací vyplývá, že nejvhodnějším médiem pro turistickou kartu je čipová karta.

1.1 Historie elektronických karet

Počátky elektronické karty se datují od roku 1970. O prvenství se vedou spory mezi Němcem Jürgenem Dethloffem, Francouzem Rolandem Morenem a Japoncem Kunitakou Arimurou.

K prvnímu masovému nasazení došlo v roce 1983 ve Francii, jednalo se o telefonní kartu *Télécarte*. Na počátku se ovšem jednalo pouze o velmi jednoduché kontaktní paměťové karty, které sloužily pouze k ukládání dat ve velmi omezeném rozsahu. Komunikaci s vnějším zařízením zajišťovaly kovové kontakty vyvedené na povrch karty.

Na konci 80. let se objevily kontaktní čipové karty. Karty už kromě paměťových obvodů obsahovaly také integrovaný mikroprocesor, který umožňoval realizovat vyspělou komunikaci mezi kartou a čtecím zařízením a hlavně kryptograficky zabezpečenou komunikaci a přístup k uloženým datům. Jednalo se však stále o kontaktní kartu – pro práci s ní bylo nutné zasunout ji do čtecího zařízení.[2]

1.2 Přehled identifikačních prvků

V podkapitole jsou uvedeny běžně známé a používané identifikační prvky, i když je pochopitelně možné vyrobit také nestandardní prvky, zvyšující bezpečnost (a samozřejmě také cenu) různými technologickými cestami a kombinacemi použitých technologií. Diplomová práce se zaměřuje na čipovou kartu, ostatní identifikátory jsou zde vypsány jen pro porovnání.

Typy identifikačních prvků:

- Čárový kód - vhodný pro identifikaci výrobků nebo zboží s cílem zjednodušit zadávání druhu zboží do počítače nebo do pokladny. Čárový kód je považován za nejlevnější a nejúčinnější technologii, dále je specifikován snadnou výrobou. Negativem je snadná výroba padělku – postačí běžná kopírovací technika. Pro systémy ověřování je nevhodný, s výjimkou míst, kde omezená životnost, nízká výrobní cena a lokální nedostupnost duplikační techniky dělají výrobu falzifikátu nezajímavou (kódy na zboží nebo časově omezený vstup na sportoviště – bazény, lyžařské areály, atd.). [3]
- Magnetický záznam - informace je zapsána na některé ze stop v magnetické vrstvě. Princip záznamu je stejný jako u magnetofonových kazet nebo počítačových disket. Výhodou těchto médií je relativně nízká cena. Nevýhodou je pak relativně snadná

[2] EFFING, W.; RANKL, W. *Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards*, München, 2008

[3] RAK, R. *Biometrie a identita* člověka *ve forenzních a komerčních aplikacích*, Praha, 2008

duplikovatelnost a malá datová kapacita záznamu. Je běžně používán např. na parkovištích nebo na platebních kartách.[4]

- Čipové karty – široká škála karet osazených čipem, obsahujícím buď jednorázově zapisovatelnou paměť (WORM) nebo přepisovatelnou paměť (EEPROM). Přístup k této paměti může být volný, přes zabezpečovací obvody (založené na symetrickém klíči) nebo karta obsahuje mikroprocesor. Čipové karty se používají v různých prostředích. Jsou vyráběny od nejjednodušších a nejlevnějších až po drahé a velmi bezpečné. Často jsou osazeny pro tento účel vyráběným mikroprocesorem, který řídí komunikaci mezi snímačem a kartou a je schopen též provádět šifrování komunikace a ověřování platnosti karty. Jako identifikační prvky pro ověřování jsou velmi vhodné, dají se využít též jako elektronické peněženky nebo pro uložení osobních dat. Nevýhodou je nutnost kontaktního snímání, které výrazně omezuje životnost karty. Mikroprocesor může obsahovat ještě kryptočip, který uchovává specifické identifikační znaky (např. digitální certifikát nebo biometriky jako otisk prstu či obraz sítnice oka) nositele karty a zajišťuje nebo výrazně urychluje identifikaci, autorizaci, šifrování a elektronické podepisování.[5]

Obrázek 1: Čipová karta

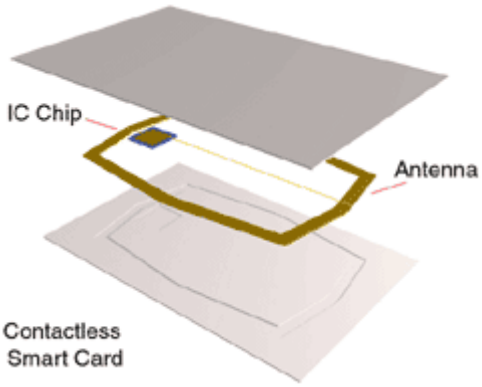
Zdroj: http://www.idwholesaler.com

- Bezkontaktní technologie - patří mezi nejdynamičtěji se rozvíjející technologie. K přenosu informace mezi snímačem a identifikačním prvkem se používá vysokofrekvenční elektromagnetické pole. Výhoda bezkontaktní technologie

[4] PANDATRON – Elektrotechnický magazín. *Karty s magnetickým pruhem* [online]. 2008

[5] JUŘÍK, P. *Svět platebních a identifikačních karet*, Praha: Grada, 2001

spočívá zejména v bezdotykovém přenosu dat, a to i bez přímé viditelnosti (např. karta v peněžence). Snímače jsou uzavřené a neobsahují žádné pohybující se mechanické části - jsou tedy výrazně odolnější jak proti vlivům prostředí, tak proti vandalizmu. Jejich další výhodou je (narozdíl od karet kontaktních) téměř nulové opotřebení při aplikaci. Bezkontaktní technologie jsou proto vhodné všude tam, kde je zapotřebí rychlého vyřízení a častého, masového využívání karty. Původně jednodušší čipy se již dnes srovnávají s čipy používanými v kontaktním světě.
Nejnovější čipové karty jsou již malým počítačem, včetně svého programovacího jazyka a operačního systému. Nevýhodou bezkontaktních technologií je zejména existence více technologických řešení, standardů a norem, které často nejsou vzájemně slučitelné. [6]

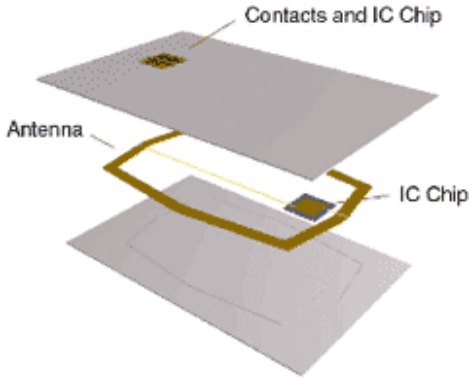


Obrázek 2: Bezkontaktní čipová karta
Zdroj: http://www.idwholesaler.com

Duální a hybridní technologie – kontaktní a bezkontaktní karty se začínají prolínat a čím dál tím častěji se na trhu objevují karty jak s kontaktní, tak bezkontaktní částí. Jedná se o karty:

- hybridní – bezkontaktní část je oddělena od kontaktní. Jsou to v podstatě „dvě karty v jedné“. Kontaktní část je osazena mikroprocesorem a bezkontaktní jen pamětí. Části nejsou nijak propojeny a nemohou spolu komunikovat.

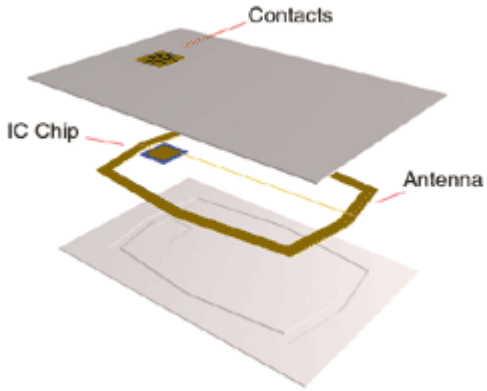
[6] JUŘÍK, P. *Svět platebních a identifikačních karet*, Praha: Grada, 2001



Obrázek 3: Hybridní čipová karta

Zdroj: http://www.idwholesaler.com

- duální – obsahují jeden obvod, nejčastěji mikroprocesor, který řídí oba dva komunikační kanály – kontaktní i bezkontaktní. Tento způsob řešení je ideální pro typickou městskou kartu s elektronickou peněženkou, kde kontaktní rozhraní slouží pro její dobíjení a bezkontaktní pro provádění jednotlivých plateb.[7]



Obrázek 4: Duální čipová karta

Zdroj: http://www.idwholesaler.com

- Technologie RFID (Radio Frequency Identification) – identifikátor navržený (nejen) k identifikaci zboží, navazující na systém čárových kódů. Stejně jako čárové kódy slouží k bezkontaktní komunikaci na krátkou vzdálenost. Čipy se dělí na aktivní a pasivní. Aktivní čipy jsou složité (obsahují zdroj napájení) a nákladné, a proto nejsou moc rozšířené. Využívají se pro aktivní lokalizaci. Pasivní čipy přijímají elektromagnetické pulsy od vysílače (čtečka), tuto energii využijí k dobití kondenzátoru a odešlou odpověď. Využívají se například pro řízení přístupu osob

[7] JUŘÍK, P. *Svět platebních a identifikačních karet*, Praha: Grada, 2001

do uzavřených objektů, identifikaci zboží, elektronické peněženky (obsahují dodatečnou paměť, do které lze zapisovat informace).[8]

- Technologie NFC (Near Field Communication) – komunikační technologie sloužící k bezdrátové komunikaci mezi elektronickými zařízeními na krátkou vzdálenost (do 20cm) nebo dotyk. Je primárně určena pro využití v mobilních telefonech. Technologie NFC je rozšíření standardu ISO/IEC 14443 (bezkontaktní karty, RFID), který kombinuje rozhraní čipových karet a bezdrátového komunikačního zařízení. NFC umožňuje spotřebitelům například provádět bezkontaktní transakce, přístup k digitálnímu obsahu a připojení přístrojů s jednoduchostí jediného dotyku.[9]

Tabulka 1: Tabulka s technickými parametry NFC, RFID, IrDa a Bluetooth

	NFC	RFID	IrDa	Bluetooth
Set –up time	<0.1ms	<0.1ms	~O.5s	~6 sec
Range	Up to 10cm	Up to 3m	Up to 5m	Up to 30m
Usability	Human centric Easy, intuitive, fast	Item centric Easy	Data centric Easy	Data centric Medium
Selectivity	High, given, security	Partly given	Line of sight	Who are you?
Use cases	Pay, get access, share, initiate service, easy set up	Item tracking	Control & exchange data	Network for data exchange, headset
Consumer experience	Touch, wave, simply connect	Get information	Easy	Configuration needed

Zdroj: http://mobilizujeme.cz

V tabulce uvedené výše jsou patrné rozdíly mezi jednotlivými technologiemi. Technologie NFC snímá na mnohem kratší vzdálenost než technologie infračerveného portu. Technologie NFC má oproti ostatním technologiím uvedeným v tabulce širší spektrum využití. Je možné pomocí této technologie platit, umožnit přístup, sdílet data, má jednoduché nastavení. Například technologie RFID (Radio Frequency Identification) je ve většině případů určena pro identifikaci zboží. Průměrná doba nastavení Bluetooth je

[8] FINKENZELLER, K. *RFID Handbook,* Chichester: John Wiley & Sons, Ltd., 2003

[9] DONOVAN, J. *Portable Electronics: World Class Designs.* Burlington: Elsevier Inc. 2009

6 sekund, technologie NFC výrazně zkracuje dobu nastavení již od 0,1ms. Přesto, že je diplomová práce zaměřena na čipové karty, je nezbytně nutné se zmínit o této nové a v budoucnu velmi rozšířené technologii NFC.

1.3 Využití čipových karet v jednotlivých oblastech

V oblasti finanční jsou využívány především karty s magnetickým proužkem, začínají se však výrazně prosazovat procesorové karty s kontaktním rozhraním pro jejich spolehlivost a bezpečnost. Bankomaty jsou dnes schopné pracovat s čipovými kartami s kontaktním rozhraním. Pro placení u obchodníka nebo při výběru z bankomatu nemá dnes bezkontaktní technologie velký význam.

V oblasti dopravy a docházkových systémů se běžně používají bezkontaktní technologie, především pro jejich vysokou odolnost proti opotřebení a vandalismu. Pokud je karta používána pouze pro systém mikroplateb za hromadnou dopravu či např. parkování, není nutné kartu vybavovat kontaktním rozhraním. Vzhledem k menším bezpečnostním požadavkům a požadované nízké ceně řešení se většinou využívá pouze paměťové karty bez vlastní inteligence (bez procesoru). Při kombinaci s jiným řešením však paměťová karta již nestačí. Proto bývá využita podle stupně bezpečnosti buď hybridní karta (kontaktní procesorová část pro řešení např. identifikace, bezkontaktní paměťová pro odečet bodů nebo pro docházkový systém) nebo duální procesorová karta.

V oblasti identifikace a autentizace se používá buď kontaktní, nebo bezkontaktní technologie. Karta je mikroprocesorová, většinou s podporou kryptoprocesoru pro podporu digitálních certifikátů a infrastruktury PKI (Public Key Infrastructure)[10]. V případech potřeby vysokého zabezpečení se používají procesorové karty s podporou biometriky (kontrola otisků prstů, sítnice oka či jiného jednoznačného biologického identifikátoru držitele karty).

[10] PKI - v kryptografii označení infrastruktury správy a distribuce veřejných klíčů z asymetrické kryptografie. PKI umožňuje pomocí přenosu důvěry používat cizí veřejné klíče a ověřovat jimi elektronické podpisy bez nutnosti jejich individuální kontroly.

1.3.1 Specifikace služeb využívajících turistickou čipovou kartu

Odbavovací systémy

Nejmasivnější použití čipových karet s bezkontaktním rozhraním je ve veřejné dopravě. Dle současné legislativy je možné využít čipovou kartu jako jízdní doklad. Čipová karta splňuje veškeré náležitosti jízdního dokladu uvedené v §5 vyhlášky MD č. 175/2000 Sb., o přepravním řádu pro veřejnou drážní a silniční osobní dopravu, tj.

- obchodní jméno dopravce, který uzavírá přepravní smlouvu
- nástupní a výstupní stanici nebo přepravní pásmo
- výši jízdného, druh jízdného, případně výši slevy
- údaj o platnosti
- další údaje umožňující kontrolu platnosti a správnosti jejího použití.[11]

Rychlé odbavení cestujícího je určeno bezkontaktním rozhraním karty a je vhodné i pro použití v MHD při nástupu předními dveřmi. Odbavovací systémy využívají funkce elektronické peněženky a vzhledem k nízké výši plateb i počtu subjektů podílejících se na provozu systému je možné je provádět na bezkontaktním rozhraní.

Elektronická peněženka

Elektronická peněženka je zásadní a nejvýznamnější aplikací na čipové kartě. Využívá se při ní paměti v čipu a některé nativní funkce (přírůstky/úbytky). Elektronickou peněženku lze využít při placení parkovného v parkovacích automatech, v jiných prodejních automatech, trafikách, stáncích s občerstvením nebo restauracích. Vyúčtování mezi všemi těmito subjekty by provádělo zúčtovací centrum zřízené v souladu se zákonem.

Rezervační systém

Službu lze využít v mnoha institucích poskytujících placené služby pro své zákazníky. Jedná se například o kina, divadla, zábavní parky, sportovní střediska apod. Nabízí se

[11] Ministerstvo dopravy České republiky: Legislativa - silniční doprava - §5 vyhlášky MD č. 175/2000 Sb., [online]. 2006

například napojení na on-line rezervační systém vstupenek, který je možné jednoduše propojit s databází čipové karty zřízením tzv. rezervačních účtů vázaných na číslo karty. Rezervace autorizované přes tento účet jsou jednoznačně identifikovatelné a mají tak vyšší bonitu. Pořadatelé tak mohou umožnit držitelům těchto karet např. rezervaci až do začátku představení. Zároveň je takto prodaná vstupenka vázána na konkrétní reálnou osobu, což umožní personalizovat nabídky návštěvníkům dle jejich většinového zájmu (např. formou direct e-mailu o novinkách, premiérách apod.).

Stravovací systém

Stravovací systém je typickou aplikací využívající kreditního způsobu placení za služby. V rámci stravovacího systému zabezpečeného prostřednictvím bezkontaktních čipových karet rozeznáváme tyto základní typy:

- On-line objednávkový systém: čipová karta je využita ve své identifikační funkci. Držitel se pomocí karty identifikuje při objednávce stravy a posléze při výdeji. Peněžní prostředky nejsou vedeny na kartě, nýbrž v on-line stravovacím systému provozovatele. Karta zaměstnance v tomto případě nahrazuje stravenky. Tento typ služby však turistická čipová karta nevyužívá.
- Restaurační systém: Umožňuje bezhotovostní platbu stravy čipovou kartou z elektronické peněženky u pokladen. Jednotlivá restaurační zařízení nemusí být propojena on-line a čerpání služeb se zapisuje na čipovou kartu. Tento typ placení za pomoci turistické čipové karty je možné využít. Nejčastějším typem platby bude platba, například v různých zábavních centrech, kde si návštěvník objedná nápoj, dluh se zapíše na čipovou kartu a návštěvník při vracení karty dluh vyrovná.

Přístupový systém

Systém, který kromě evidence transakcí blokuje či naopak povoluje vstup do určitých zón s řízeným přístupem. Čipová karta v tomto případě nahrazuje několik klasických klíčů. Poskytuje rychlé a komfortní ovládání dveří, turniketů a závor. V případě turistické karty lze využít pro vstupy do areálů nebo sportovišť.

Slevové a věrnostní programy

Pro zvýšení atraktivity služeb je vhodné začlenit do systému tzv. věrnostní programy. Věrnostní programy umožňují držet o zákazníkovi značné množství informací

(preferovaná lokalita pobytu, ubytovací zařízení, sportoviště, areály, atrakce, památky apod.). Na základě takto získaných informací lze změnit strategii propagace méně preferovaných lokalit, památek atd. například zavedením slevových akcí.

1.4 Specifikace služeb a požadavků na turistickou kartu

Primárně je nutné vybrat služby a nadefinovat požadavky, které má turistická karta splňovat, aby bylo možné vybrat vhodné technologické řešení, které bude vhodně kombinovat HW a SW stránku projektu a poskytovat komplexní a ucelenou službu turistům.

Čárový kód má oproti dalším systémům značnou nevýhodu v tom, že není umožněna přímá platba za služby bezkontaktní technologií bez objednání či vygenerování dalšího unikátního kódu. Naopak čipová karta nebo technologie NFC umožňují platbu online za jakoukoli službu, kterou se návštěvník rozhodne využívat bez nutnosti jejího objednání. Jde o princip elektronické peněženky, na kterou lze poskytovat slevu (částečnou nebo úplnou). Z hlediska bezpečnosti je čárový kód rovněž lehce manipulovatelný, karty a NFC technologie zabezpečené PINem umožňují vyšší zabezpečení služeb.

Tabulka 2: Popis požadovaných služeb a jednotlivých technologií

Služba	Čárový kód	Čipová karta, magnetická karta, RFID	Mobilní telefony, NFC
Platba jízdenek MHD	NE	ANO	ANO
Nákup jízdenek skibusů, cyklobusů	NE	ANO	ANO
Poskytování slev v rámci slevového systému (v rámci provádění plateb)	ANO	ANO	ANO
Přímá platba za jízdenky na lanovky a vleky	NE	ANO	ANO

Přímá platba za hotel a hotelové služby (lze propojit se vstupem do pokojů, sauny, bazénu, ...)	NE	ANO	ANO
Přímá úhrada parkovného u turistických atrakcí	NE	ANO	ANO
Nákup služeb cestovního ruchu kulturního zaměření – koncerty, vstupy do muzeí apod.	NE	ANO	ANO
Nákup služeb cestovního ruchu sportovního zaměření – aqvapark, bobová dráha, hřiště apod.…	NE	ANO	ANO

Zdroj: Studie technického řešení digitalizace Olomouc region Card

Tabulka výše znázorňuje požadované služby a jednotlivé možné technologie pro turistickou kartu. Z tabulky je patrné, že technologie čárového kódu je nedostačující pro požadavky turistické karty. Diplomová práce je zaměřena na čipové karty, které jsou pro zmíněné požadavky dostačující. Aby však bylo možné využívat všechny zmíněné služby, je nutné zvolit takový typ čipové karty, která umožní nabíjení kreditu na kartu k možnosti placení, případně propojení přímo s bankovními produkty.

1.5 Standardizace a normalizace v oblasti čipových karet

Normativní parametry karet definuje jednoznačně rodina norem ISO 781x. Jsou definovány rozměry karty, odolnost a konkrétně v normě ISO 7816 i parametry

kontaktního rozhraní karty včetně definice komunikačních protokolů. Tyto normy jsou převzaty i do ČSN (v tomto případě konkrétně do ČSN 27816).

Kontaktní rozhraní karty je touto normou definováno již dlouhou dobu, takže dnes již v podstatě neexistuje karta s kontaktním rozhraním, které by uvedené normy ISO 781x nesplňovala. Naproti tomu pro bezkontaktní rozhraní existuje mnoho různých řešení.

V pásmu nízkých kmitočtů (od 100 kHz) existuje mnoho řešení a průmyslových „skorostandardů“. Vzhledem k pomalému přenosu je většinou využíváno pouze čtení pevných dat z identifikačního členu. Používají se většinou pro interní řešení identifikace a docházkových systémů, pro sofistikovanější aplikace nejsou vhodné.

Jsou definovány tři normy ISO, všechny definované pro pásmo středních kmitočtů (13,59 MHz). Jedná se o tyto normy:

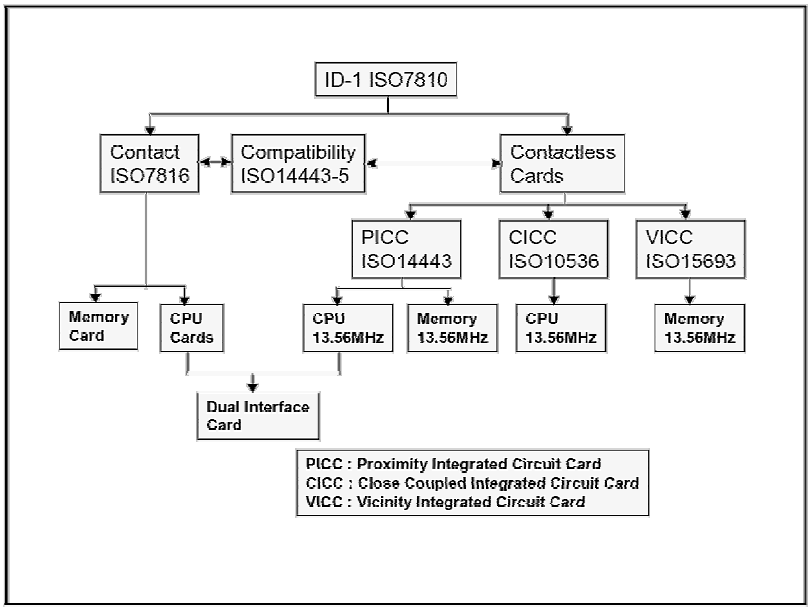
- ISO/IEC 10536 (close coupled cards, CICC) definuje bezkontaktní rozhraní karty pracující do cca 2 mm vzdálenosti („skorodotykové karty“). Norma byla původně zamýšlena pro bankovní aplikace s důrazem na bezpečnost, nedosáhla však většího rozšíření v praxi a nyní se od ní upouští.
- ISO/IEC 14443 (proximity range cards, PICC) je nejrozšířenější a nejpoužívanější norma pro bezkontaktní karty, definuje rozhraní fungující do cca 10 cm. Norma není zcela jednotná, připouští dvě hlavní varianty – ISO/IEC 14443A (v čele s technologií Philips MIFARE) a ISO/IEC 14443B (např. rodiny čipů Motorola, Infineon) lišící se komunikačním protokolem a způsobem přenosu dat. Drtivá většina dnes vyráběných čtecích zařízení je však schopna číst obě normy. Rozšířením tohoto standardu je technologie NFC.
- ISO/IEC 15693 (vicinity range cards, VICC) – technologie, pracující do vzdálenosti 1,2 m, která byla původně určena především pro hromadnou identifikaci předmětů, např. dílů ve výrobě, při zpracování zavazadel na letištích atd. Dnes se začíná prosazovat i v oblasti identifikace osob.

Většina řešení odbavovacích systémů v dopravě, identifikace osob a lokálních projektů elektronických peněženek (nebankovních institucí) využívá buď karty postavené

na bezkontaktní technologii ISO/IEC 14443 (A nebo B), nebo kombinaci bezkontaktní (ISO/IEC 14443) a kontaktní (ISO/IEC 7816) technologie v podobě hybridních nebo duálních karet. Touto cestou jde i většina projektů městských čipových karet v Evropě.

Výjimkou jsou projekty, které se snaží určit si svoji vlastní normu. Příkladem může být německo-švýcarský projekt elektronické vlakové jízdenky EasyRide. Proto doporučujeme držet se stávajících norem, které se již v praxi osvědčily a zvolit duální kartu, postavenou na normách ISO/IEC 7816 a ISO/IEC 14443A (v ČR je asi nejvíc rozšířena technologie MIFARE, tj. ISO/IEC 14443A).[12]

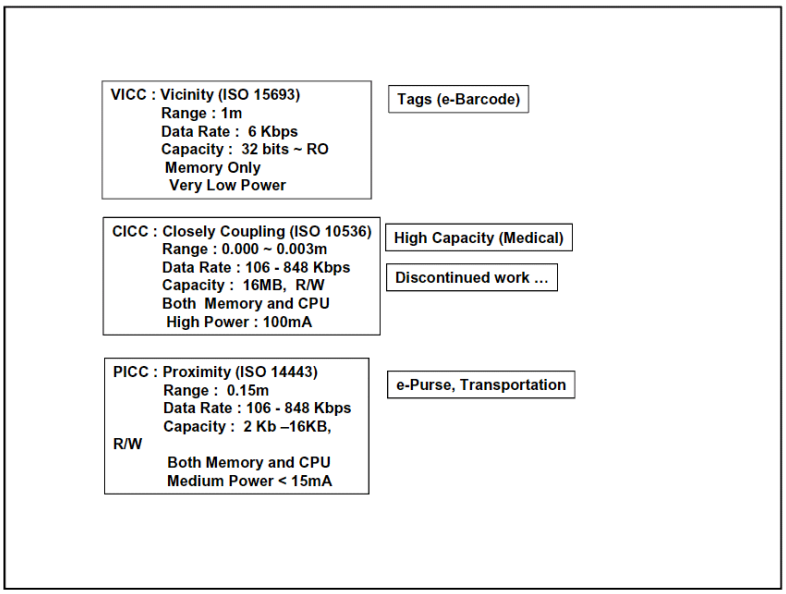
Následující obrázky přehledně ukazují souvztažnosti jednotlivých norem týkajících se čipových karet a srovnání základních parametrů jednotlivých norem pro bezkontaktní karty. První obrázek znázorňuje rozvětvení norem kontaktních a bezkontaktních čipových karet. Druhý obrázek znázorňuje schéma druhů bezkontaktních čipových karet a jejich využití – PICC je využívána pro elektronické peněženky, v hromadné dopravě, CICC se vyznačuje vysokou kapacitou (až 16MB), VICC je ze všech standardů nejméně výkonná (kapacita jen 32b) a nelze na ní zapisovat data, je jen pro čtení.



Obrázek 5: Schéma norem kontaktních a bezkontaktních čipových karet

Zdroj: Specifikace média pro městské čipové karty, Liberecká IS,a.s.

[12] POPELKA, P. VIMR, M. *Systém městské čipové karty pro město Plzeň*, 2003



Obrázek 6: Schéma norem bezkontaktních čipových karet

Zdroj: Specifikace média pro městské čipové karty, Liberecká IS, a.s.

1.6 Technologie MIFARE

Nejvíce rozšířenou technologií platebních a bankovních karet na světě je v současnosti MIFARE vyvíjená společností NXP Semiconductors, která se v roce 2006 oddělila od společnosti Philips Electronics. Na počátku roku 2006 fungovalo ve světě více než 500 milionů karet této rodiny a 5 milionů komunikačních zařízení. Technologie MIFARE má otevřenou architekturu, takže výrobců karet je více než 50 a výrobců čteček přes 200.

Přehled typů karet MIFARE:

- MIFARE Ultralight
- MIFARE Standard (Classic)1k
- MIFARE Standard (Classic) 4k
- MIFARE DESFire
- MIFARE PROX

• MIFARE SmartMX[13]

Novinkou je MIFARE Ultralight C představený na veletrhu průmyslu Cartes v roce 2008, MIFARE Ultralight C je součástí nízkonákladové nabídky NXP. Díky rozšířenému standardu umožňuje snadnou integraci do stávající infrastruktury. Využívá metodu šifrování 3DES[14]. Klíčové aplikace pro MIFARE Ultralight C jsou veřejná doprava, vstupenky, věrnostní karty.

Náhradou za MIFARE Standard 1k, 4k je MIFARE Plus. Správa dat je identická jako u MIFARE Standard. MIFARE Plus však využívá metodu šifrování AES (Advanced Encryption Standard)[15], která je bezpečnější než dosavadní CRYPTO1.

Další novinkou je technologie MIFARE SAMs (Secure Access Modules) - nejsou to však bezkontaktní čipové karty. MIFARE SAMs jsou bezpečné přístupové moduly, jejichž účelem je zajistit bezpečné uložení šifrovacích klíčů a šifrovací funkce pro terminály, které umožňují bezpečný přístup k Mifare produktům a umožňují bezpečnou komunikaci mezi terminály a hostitelem.[16]

---

[13] Palán, M. *Bezkontaktní čipové karty Českých drah*. Vědeckotechnický sborník ČD č.21/2006. [online]. 2006

[14] Bloková symetrická šifra, která nahrazuje starší verzi DES. 3DES využívá stejný algoritmus jako DES, kvůli zpětné kompatibilitě, avšak dvohnásobný, či trojnásobný klíč (112b nebo 168b)

[15] AES je platnou alternativou algoritmu DES, přijatý v roce 2002. Tento algoritmus využívá délu bloku 128b a podporuje tři délky klíče 128, 192 a 256 bitů, AES nemá slabé klíče a je odolný proti útokům a metodám lineární a diferenciální kryptoanalýzy.

[16] NXP, *Mifare Type Identification Procedure*. [online]. 2009.

Tabulka 3: Technické parametry technologie MIFARE

	MIFARE Ultralight	MIFARE Standard 1k	MIFARE Standard 4k	MIFARE DESFire	MIFARE PROX	SmartMX
velikost paměti	64 B	1024 B	4096 B	4096 B	16384 B	73728 B
délka čísla karty	56 bitů	32 bitů	32 bitů	56 bitů	56 bitů	56 bitů
počet zápisů do paměti	1000	100.000	100.000	100.000	100.000	100.000
doba uchování dat	2 roky	10 let	10 let	10 let	10 let	10 let
doba vykonání typické transakce	31,4 ms	164 ms	164 ms	105 ms	105 ms	105 ms
elektronická peněženka	není	32 bitů, plný kredit	32 bitů, plný kredit	plný i omezený kredit	Uživatelsky programovatelná	Uživatelsky programovatelná
metoda šifrování dat	žádná	CRYPT1	CRYPT1	DES, 3DES AES*	DES, 3DES, RSA	DES, 3DES, RSA, ECC
počet aplikací	1	16	40	28		
vhodné použití	jednorázové jízdenky	jednoduchá elektronická peněženka pro drobné platby, časová jízdenka	jednoduchá elektronická peněženka pro drobné platby, časová jízdenka	e-ticketing, věrnostní programy, elektronická peněženka	e-business	e-business

Zdroj: http://www.cdrail.cz/vts/CLANKY/vts21/2108.pdf

Tabulka výše popisuje technické parametry technologie MIFARE. Jsou zde uvedeny metody šifrování dat, velikost paměti, doba uchování dat, vhodné využití atd. Z jednotlivých parametrů uvedených v tabulce se zdá pro funkci turistické karty nejvhodnější MIFARE DESFire. Umožňuje rezervační služby na vstupenky, věrnostní a slevové programy a co je nejdůležitější, umožňuje funkci elektronické peněženky.

Karty MIFARE PROX a SmartMX jsou vyspělé duální procesorové karty (s kontaktním i bezkontaktním rozhraním), jejichž funkce lze programovat v jazyce JAVA. Umožňují tak naprogramování složitých a velmi bezpečných aplikací s širokým spektrem použití. Jsou charakteristické vysokou výrobní náročností, vysokou cenou (asi osminásobná oproti MIFARE Standard 1K a pětinásobná oproti MIFARE DESFire) a komplikovanějším vytvářením softwaru.

Karta MIFARE Ultralight dokáže pouze jedinou aplikaci. Pro svou malou paměťovou kapacitu, velmi nízkou bezpečnost, krátkou trvanlivost a na druhé straně také nízkou cenu je vhodná například pro jednorázové, případně celodenní jízdenky.[17]

1.6.1 Karty MIFARE DESFire

Karty typu MIFARE DESFire se nejlépe hodí pro plnění funkce turistické karty, proto jsou v práci popsány podrobněji než ostatní typy karet MIFARE. Karty MIFARE DESFire mají následující parametry:

Radiofrekvenční rozhraní

- bezkontaktní přenos dat, napájení elektromagnetickým polem (provoz bez baterií)
- provozní vzdálenost až 100 mm (v závislosti na geometrii antény a výkonu vysílače)
- provozní frekvence 13,56 MHz
- přenosová rychlost 106 kbit/s, 212 kbit/s nebo 424 kbit/s
- integrita dat: 4 Byte MAC (message authentication code), 16 bit CRC, parita, bitové kódování, bitový počet
- antikolizní vlastnosti (možnost práce více karet současně v poli antény)
- přenosový protokol dle ISO 14443-4

Stálá paměť

- 4 KB stálé (nonvolatilní, udržující si obsah i bez přítomnosti napájecího napětí) paměti, v nové verzi až 8 KB

[17] Palán, M. *Bezkontaktní čipové karty Českých drah*. Vědeckotechnický sborník ČD č.21/2006. [online]. 2006

- doba zápisu 2 ms na blok (1 ms mazání předchozích dat, 1 ms vlastní zápis)
- doba uchování dat 10 let
- trvanlivost 100 000 zapisovacích cyklů

Organizace stálé paměti

- flexibilní souborový systém (u starších typů karet se používaly paměťové bloky o pevné velikosti)
- až 28 zcela nezávislých aplikací na kartě
- až 16 souborů pro každou aplikaci
- až 14 kryptografických klíčů pro každou aplikaci

Bezpečnost

- 7-bytové jedinečné číslo karty
- 3-kroková autentifikace (viz níže)
- hardwarově podporované šifrování algoritmy DES/3DES (v nové verzi i AES)
- zabezpečení dat 4-bytovým MAC (Message authentication code)
- autentizace na aplikační úrovni

Výhody oproti MIFARE Standard

- plně multiaplikační systém, každou z aplikací má její vlastník plně pod kontrolou
- větší paměť (dána lepším využitím paměti)
- výrazně rychlejší čtení a zápis
- předpoklad rozvoje do budoucna s kompatibilním protokolem ISO 14443-4

• významně dokonalejší kryptografické zabezpečení (3DES)

Každou nezávislou aplikaci na kartě reprezentuje její identifikátor AID o délce 3 byte (Application Identifier). Soubory mohou být pěti typů: standardní datový soubor, záložní datový soubor, hodnotový soubor se zálohou, soubor s lineárním záznamem a soubor s cyklickým záznamem (oba se zálohou). Zálohou je automaticky vybaveno prvních 8 souborů každé aplikace, zbylých 8 je bez zálohy.

Data se mezi kartou a čtečkou mohou přenášet ve 3 režimech: nezašifrovaně, nezašifrovaně se zašifrovaným autentizačním kódem (MAC) a zašifrovaně.

Přístup k datům je možný na aplikační úrovni. Pro každou aplikaci lze stanovit až 14 různých klíčů, které mohou různým subjektům zajistit různý stupeň přístupu k datům. Pro každý klíč pak lze stanovit jedno ze čtyř oprávnění: čtení dat, zápis dat, čtení i zápis a změna oprávnění k přístupu.

Kromě těchto klíčů existuje pro každou aplikaci ještě tzv. master klíč (Application Master Key), který je vždy vyžadován pro operace změny nastavení přístupových práv aplikace a změny master klíče aplikace. Dále jeho znalostí mohou být podmíněny některé další operace, jako vytvoření a zrušení souboru, čtení seznamu souborů a čtení přístupových práv aplikace.

Třetím typem klíče je master klíč karty (PICC Master Key). Ten je nezbytný pro formátování karty, změnu nastavení přístupových práv ke kartě a ke změně master klíče karty. Navíc může být vyžadován pro další operace, jakými jsou vytvoření a zrušení aplikace, čtení seznamu aplikací a čtení přístupových práv karty.

Autentizace je proces, který proběhne na začátku komunikace karty se čtečkou. Při této proceduře se čtecí zařízení a karta navzájem ujistí, že je jim známa hodnota tajného klíče, aniž by si hodnotu tohoto klíče navzájem posílaly. Vedlejším produktem tohoto procesu je

hodnota tzv. session key (klíč platný pouze pro tuto jednu komunikaci), který se poté využije pro šifrování přenášených dat.[18]

[18] Palán, M. *Bezkontaktní čipové karty Českých drah*. Vědeckotechnický sborník ČD č.21/2006. [online]. 2006

2. Používaná zařízení a jejich funkce pro práci s daty a komunikaci karty s okolím

Kapitola popisuje konkrétní zařízení pro snímání čipových karet, v případě diplomové práce turistických čipových karet. U každého zařízení jsou popsány i jeho funkce. Podrobněji jsou v této kapitole rozepsána zařízení, která se využívají v městské dopravě. Na turistickou čipovou kartu má návštěvník možnost si zakoupit jízdenku v automatu, pokud má nabitou elektronickou peněženku, nebo si může zakoupit předplatné na určitý počet dnů, které je možné zkontrolovat čtečkou revizora nebo terminálem pro čtení čipových karet. Dalšími zařízeními popisovanými v této kapitole jsou bankomaty a terminály, které mají funkci nabíjení peněz do elektronické peněženky.

2.1 Bankomaty, terminály

Bankomaty (ATM) a platební terminály prodejců (POS), které jsou schopné přijímat čipové karty, obsahují několik tzv. Security Access Module (SAM) pro každou kartu, se kterou má ATM nebo POS komunikovat. SAM zajišťuje prvotní ověření karty a obsahuje popis komunikace s kartou („návod jak s kartou zacházet“).

Aby bylo po technické stránce možné využít městskou kartu v konkrétním bankomatu, platebním terminálu či jiném terminálu postaveném na podobné koncepci, musí tento obsahovat odpovídající SAM. Dodavatelem SAM je provozovatel karetního systému, případně jeho smluvní partner, který řešení vyvíjí a dodává. Bankomaty by měly primárně sloužit k on-line dobíjení elektronických peněženek z účtu. Je možné do bankomatů časem přidat i další funkcionalitu, pokud se banky podaří přesvědčit o výhodnosti takové změny.

Podobně fungují také multifunkční terminály. Typickým příkladem je IQ Terminal. Jsou navržené jako univerzální terminály, které umožňují práci s čipovými kartami. Nabízejí uživateli mnohem větší spektrum operací s kartou a dobíjení elektronické peněženky může být jednou z nich. Dalšími funkcemi mohou být prohlížení obsahu karty, platby za vybrané městské služby, nákup předplatného na hromadnou městskou dopravu atd.

Aby mohly multifunkční terminály nabízet tyto funkce, je nutné, aby tuto funkcionalitu podporovalo kartové a zúčtovací centrum.[19]

2.1.1 Čtečka čipových karet – CKC

Zařízení slouží pro obousměrnou komunikaci mezi bezkontaktní čipovou kartou a PC. Umožňuje zapisovat a vyčítat data z bezkontaktních čipových karet typu MIFARE Standard a MIFARE DESFire prostřednictvím PC vybaveného příslušným SW. Vestavěné LED kontrolky signalizující stav zařízení.[20]

Čtečkou čipových karet je možné vybavit například také rotační turnikety, které zajišťují kontrolu vstupu. Čtečka je využívána například pro stravovací nebo docházkové systémy.

Obrázek 7: Čtečka čipových karet – CKC

Zdroj: http://www.mikroelektronika.com

2.2 Mobilní automaty pro městskou dopravu

Podkapitola popisuje různé druhy zařízení pro odbavování cestujících pomocí čipových karet v městské dopravě. Jsou zde popsána běžně používaná zařízení jako zařízení pro odbavování cestujících pomocí bezkontaktních čipových karet CAMEL nebo CARDMAN. Dále mobilní automat na výdej jízdenek AVJ F, kde je možné si zakoupit jízdenku nabitou

[19] POPELKA, P. VIMR, M. *Systém městské čipové karty pro město Plzeň*, 2003

[20] Mikroelektronika, *Odbavovací systémy.* [online]. 2009

čipovou kartou (elektronická peněženka). Je zde popsána také kontrolní čtečka čipových karet pro revizora, která je pro přepravní kontrolu nezbytně nutná.

2.2.1 Mobilní automat na výdej jízdenek - AVJ F

Automat AVJ F byl navržen speciálně pro provoz v prostředcích hromadné přepravy (autobusy, tramvaje, trolejbusy a vlaky). Hlavní důraz je kladen na maximální rychlost, příjemnou obsluhu uživatelem a spolehlivé vracení mincí.

Obrázek 8: Mobilní automat na výdej jízdenek - AVJ F
Zdroj: http://www.mikroelektronika.com

- Automat může pracovat jako samostatná jednotka, nebo k němu může být připojena ovládací jednotka, např. palubní počítač, externí klávesnice apod.
- Pro co nejrychlejší platbu netříděnými a nepočítanými mincemi je použit motorický podavač mincí a mincovní hlavice rozpoznávající až 12 různých typů mincí.
- Mincovní systém využívá 4 výměnné zásobníky s funkcí mezikasy a výměnnou pokladnu.
- Pro zvýšení odolnosti proti poškození a neoprávněné manipulaci je skříň automatu vyrobena z 2 mm nerezové oceli.
- Záložní baterie zajišťuje nepřerušovaný chod v případě krátkodobého výpadku napájení.

- Modulární systém umožňuje jednoduchou a rychlou výměnu specifických komponent.
- Tepelná tiskárna s ořezávačem zajišťuje vysokou rychlost při výdeji jízdenek.
- Možnost integrace čtečky bankovních a bezkontaktních čipových karet.
- Funkce automatu si může uživatel z velké části modifikovat sám s využitím počítačové aplikace dodávané výrobcem.[21]

2.2.2 Zařízení pro odbavování cestujících pomocí bezkontaktních čipových karet

Zařízení je určeno pro komfortní, rychlé a bezpečné odbavení cestujících v hromadné dopravě pomocí bezkontaktních čipových karet. Je připraveno pro práci v různých tarifních systémech včetně CHECK-IN/ CHECK-OUT. Zařízení je vestavěno do masivní, mechanicky odolné uzamykatelné skříně s moderním designem. Zařízení je vyráběno v několika provedeních: bez displeje, s malým dvouřádkovým displejem a s velkým dotykovým displejem.

Cestující může zařízení dle potřeby ovládat pomocí bezkontaktní dotykové obrazovky až s 15-ti aktivními plochami, která je realizována grafickým černobílým podsvíceným displejem. Grafický displej poskytuje cestujícím dobře čitelné, srozumitelné informace umožňující snadné a rychlé odbavení. Jedná se např. o informaci o platnosti provedené transakce, zůstatku finančního obnosu na kartě nebo časovou platnost apod. Cestující je o platnosti provedené transakce rovněž informován prostřednictvím 2 signalizačních LED, které jsou umístěny nad displejem a zvukovým signálem. Pod displejem je umístěno místo pro přikládání bezkontaktní karty.

Na základě předem připravených dat uložených v paměti provádí zařízení zpracování a záznam provedených transakcí. Zařízení může pracovat v režimu autonomním, řídícím nebo podřízeném.

Pomocí některé ze sběrnic IPIS, RS-485 nebo CAN může komunikovat s dalšími zařízeními umístěnými na palubě vozidla, číst z nich data a řídit je v případě, že je

[21] Mikroelektronika, *Odbavovací systémy.* [online]. 2009

v řídícím režimu. V řídícím režimu rovněž zabezpečuje bezdrátový přenos dat mezi palubním systémem a vozovnou. [22]

Obrázek 9: Terminál pro bezkontaktní karty
Zdroj: http://www.mikroelektronika.com

2.2.3 Zařízení pro odbavování cestujících

Zařízení typu CARDMAN má oproti typu CAMEL zabudovanou tiskárnu. Řídící jednotka s 32 bitovým procesorem a paměťovým prostorem 6 MB zajišťuje vysokou rychlost a bezpečnost při zpracování dat. Zařízení CARDMAN má velký plně grafický displej s velmi dobrou viditelností k zobrazení všech potřebných údajů v optimální velikosti. Bezkontaktní dotyková obrazovka s 15 aktivními plochami, umožní cestujícímu snadnou a rychlou volbu tarifu. Provozovateli pak dává možnost provádění operativních změn tarifní politiky výměnou SW bez zřetele na omezený počet tlačítek a výměnu popisu k nim umístěným R/W zařízení pro práci s bezkontaktními kartami MIFARE se čtecí vzdáleností do 10 cm. Výkonná tiskárna s ořezávačem s vysokou životností zajišťuje maximální rychlost a kvalitu plně grafického tisku. Flexibilita systému dovoluje plnou modifikaci funkcí a parametrů zařízení a dává uživateli možnost přizpůsobit funkce systému dle svých potřeb. Je zde možná bezdemontážní výměna firmware. Instalace je velice rychlá a snadná pomocí rychloupínacího držáku. [23]

---

[22] Mikroelektronika, *Odbavovací systémy.* [online]. 2009

[23] Mikroelektronika, *Odbavovací systémy.* [online]. 2009

Obrázek 10: Terminál pro bezkontaktní karty

Zdroj: http://www.mikroelektronika.com

2.2.4 Kontrolní čtečka revizora

Čtečka revizora je přenosné programovatelné zařízení s vestavěným snímačem bezkontaktních čipových karet. Čtečka rychle a bezkontaktně čte a ověřuje informace uložené na kartách - provádí kontrolu dat nahraných na kartě, kontrolu záznamů o přiložení k odbavovacím terminálům. Revizor přiblíží bezkontaktní čipovou kartu ke snímací ploše. Na displeji jsou zobrazeny potřebné informace jako např. jméno držitele karty, doba platnosti časového cestovního lístku (od-do), rozsah platnosti, cena časového lístku (obyčejný studentský, důchodce resp. přenosný). V paměti čtečky jsou uloženy data o denní činnosti revizora, všech zkontrolovaných karet, black list, atd. Čtečka je navíc vybavena komunikačním portem pro komunikaci s PC a konektorem pro dobíjení baterií. Pomocí komunikačního portu dochází k aktualizaci black listu, ale také k přenosu dat do PC o denní činnosti revizora. V případě, že ve čtečce nebyla, v supervizorem nastaveném časovém intervalu (např. 1 den), provedena aktualizace dat - black list atd., dojde k jejímu zablokování. Tento způsob zabezpečení zároveň zamezuje zneužití např. odcizené čtečky. V paměti čtečky jsou uloženy data o činnosti revizora, všech zkontrolovaných karet, black list, atd. [24]

[24] Mikroelektronika, *Odbavovací systémy.* [online]. 2009

3. Ochrana osobních údajů držitelů karet a související legislativa

Základním bodem zavedení turistické karty je zcela určitě ochrana osobních údajů držitelů karet. Osobní data dávají systému velkou možnost vyhodnocování chování zákazníků, je možné upravovat nabídky na míru cílové skupině, individuálně pracovat se zákazníkem, oslovovat ho v preferovaných zájmech. Stávající legislativa daná Zákonem o ochraně osobních údajů a především výklad inspektorů Úřadu pro ochranu osobních údajů vylučují jakoukoli budoucí otevřenost systému k dalším přistupujícím subjektům, protože smlouvy mezi správcem a zpracovateli osobních údajů musí být uzavírány napříč a zákazník (subjekt osobních údajů) musí při vzniku vztahu (zakoupení karty s evidencí osobních údajů) projevit informovaný souhlas, to znamená souhlas se zpracováním svých osobních údajů všem subjektům, které jeho data budou dále zpracovávat. Zpracování osobních údajů držitele karty je navrženo níže.

3.1 Návrh zpracování osobních údajů u turistické karty

Držitel karty je fyzická osoba, které provozovatel přímo nebo prostřednictvím prodejního místa kartu vydá. K vydané kartě dostane držitel karty smluvní podmínky, jejich akceptací vyslovuje souhlas, aby provozovatel v souladu s ustanovením § 5 a násl. zákona č. 101/2000 Sb., o ochraně osobních údajů, zpracovával jeho osobní údaje uvedené v žádosti o vydání karty, resp. údaje zaznamenané do karty. Pro nakládání s osobními údaji držitele karty stanoví provozovatel následující podmínky:

a) vymezení osobních údajů: jméno, příjmení, datum narození, bydliště, podrobnosti elektronického kontaktu pro elektronickou poštu, číslo telefonického kontaktu

b) účel zpracování: výkon práv a plnění povinností vyplývajících ze smluvních podmínek, statistika čerpání služeb prostřednictvím karty, vyhodnocování fungování systému turistické karty a jeho zlepšování, vyhodnocování kvality služeb akceptačních míst a její zlepšování, zpětná vazba mezi jednotlivými subjekty

c) prostředky a způsob zpracování osobních údajů: automatizovaně i manuálně v elektronické i tištěné formě

d) doba zpracování informací bude určena provozovatelem

e) osoby, kterým mohou být osobní údaje zpřístupněny: provozovatel, akceptační místa a prodejní místa

Držitel karty má právo přístupu ke svým osobním údajům, právo na opravu osobních údajů, jakož i další práva dle § 21 Zákona. Držitel karty má právo souhlas se zpracováním svých osobních údajů kdykoli písemnou formou odvolat. Provozovatel je oprávněn využít podrobnosti elektronického kontaktu držitele karty pro elektronickou poštu pro potřeby šíření obchodních sdělení týkajících se turistické karty. Provozovatel je povinen při zasílání každé jednotlivé zprávy umožnit držiteli karty jednoduchým způsobem, zdarma nebo na účet provozovatele odmítnout souhlas s takovým využitím svého elektronického kontaktu.[25]

3.2 Legislativa související s ochranou osobních údajů

Právo na důvěrnost dat je zmíněno v článku 8 Evropské konvence na ochranu lidských práv a základních svobod a také v základních principech práva EU[26]. Směrnice 95/46/EC Evropského parlamentu a konvence Rady Evropy zdůrazňuje právo na důvěrnost s ohledem na automatické zpracování dat. Směrnice 95/46/EC definuje základní rámec nakládání s osobními daty i pro implementátory a operátory systému odbavování.[27] V ČR je ochrana osobních údajů dána zákonem č. 101/2000 Sb.[28]

[25] LipnoCard. Všeobecné smluvní podmínky, [online]. 2009

[26] European Court of Human Rights. *Úmluva o ochraně lidských práv a základních svobod.* [online]. 2009

[27] Registry.cz. *Legislativní aspekty: Evropská unie.* [online]. 2009

[28] Úřad pro ochranu osobních údajů. *Zákon pro ochranu osobních údajů.* [online]. 2009

Smyslem zákona o ochraně osobních údajů je Listinou základních práv a svobod zaručené právo na ochranu občana před neoprávněným zasahováním do jeho soukromého a osobního života neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů. V současné společnosti je vlivem rozvoje informačních technologií toto právo stále více narušováno.

Zákon o ochraně osobních údajů se prolíná i do zákona o silniční dopravě a do zákona o drahách. Zákon č. 111/1994 Sb. o silniční dopravě ve znění pozdějších předpisů i Zákon č. 266/1994 Sb. o drahách umožňují vyžadovat prostřednictvím dopravcem pověřené osoby od cestujícího prokázání totožnosti, resp. poskytnutí osobních údajů. Ve vztahu k zákonu o ochraně osobních údajů je pak provozovatel služby (dopravce apod.) oprávněn použít tyto údaje pro ochranu svých práv, tj. pro vymáhání dlužného jízdného a přirážky. Ve zpracování těchto osobních údajů však není oprávněn pokračovat ve chvíli, kdy se svých práv již domohl a k dalšímu zpracování nedostal souhlas od subjektu údajů. Zákonným zpracováním osobních údajů potom tedy může být uchování účetní dokumentace podle zákona o účetnictví, nikoli však vedení evidence cestujících, kteří někdy v minulosti poskytli své osobní údaje za účelem vymáhání dlužného jízdného a přirážky.[29]

[29] Ministerstvo dopravy České republiky. *Legislativa - silniční doprava*, [online]. 2006

4. Bezpečnost bezkontaktních čipových karet

Nejen zajištění ochrany osobních údajů, ale i bezpečnost samotných čipových karet je velmi důležitá. Karta musí být zajištěna před možností falzifikace nebo před možností jakéhokoli zneužití. Ochranné prvky by měly být nakombinovány, tedy měly by být použity prvky neelektronické (hologram, vytlačené písmo, speciální barvy atd.) i elektronické. Zabezpečení je zaměřeno na jednu ze specifických aplikací městské karty a to na médium pro podporu rozvoje turistického ruchu – turistickou kartu.

4.1 Obecné ochranné prvky

Tato podkapitola popisuje zejména obecné, tedy neelektronické ochranné prvky karty jako jsou barva, rozměry, fotografie apod. Tyto prvky zčásti zajišťují bezpečnost čipové karty. Je však vhodné tyto prvky kombinovat s prvky elektronickými. Bezpečnostní požadavky na turistickou kartu budou nižší než na běžnou městskou kartu protože možná ztráta karty nepředstavuje závažné riziko zneužití nahraných finančních prostředků nebo zneužití osobních údajů.

4.1.1 Barva

Pro každý druh turistické karty je vhodné určit jinou barvu. Je na provozovateli, aby rozhodl, zda bude barevnost určována dle druhu služeb nebo dle uživatele. Barva dle uživatele bude určena různými skupinami těchto uživatelů (například dítě – modrá barva, student a senior – zelená barva a dospělý – fialová) anebo pokud by se jednalo například o kartu pro jednotlivce nebo rodinnou kartu. Obsluze v různých zařízeních a atraktivitách barva karty usnadní kontrolu u vstupu. Barva dle druhu služby by byla určena, dle toho, jestli si turista zakoupí kartu s balíčkem služeb určených jen pro vstupy nebo služeb určených pro vstupy a ubytovací zařízení apod. Karta by se mohla barevně odlišovat také dle časové platnosti – dvoudenní, týdenní apod. Barevnost karet by mohla být nakombinována i spojením zmiňovaných druhů rozlišení. V tomto případě by karty měly příliš mnoho barev a působilo by to spíše zmatečně.

4.1.2 Rozměry karty

Čipová karta pro navržený typ řešení by měla mít rozměry standardní platební karty, z důvodu dobíjení elektronické peněženky v bankomatech apod. Čipové karty se v současnosti zhotovují ve formátu EMV, na kterém se dohodly klíčové kartové asociace VISA a MasterCard. Formát karty je tedy v rozměrech cca 8,6 cm x 5,4 cm x 0,76 mm. Povolené odchylky se pohybují řádově v setinách milimetrů. Stanoveny jsou i poloměry zakřivení rohů karty, dislokace použitého mikročipu a další. Karta odlišných rozměrů není příslušným snímacím zařízením akceptována. Nesprávné rozměry karty mohou odhalit případný padělek.[30]

4.1.3 Omezení platnosti karty

Čipová karta pro podporu turistického ruchu v regionu bude mít stanovenu pevnou dobu platnosti. Záleží na provozovateli, jaké časové úseky platnosti karty zvolí. Jak již bylo zmíněno v podkapitole o zbarvení karet, mohou se karty s různými časovými úseky vyznačovat jinou barvou. Spíše však bude určena platnost karty časovým úsekem od prvního použití karty a opět záleží na provozovateli, zdali bude platnost časového úseku ukončena například u dvoudenní karty striktně za 48 hodin od prvního použití karty nebo až o půlnoci posledního dne platnosti. Platnost karty může být při příští návštěvě regionu opět aktivována. Není tedy zapotřebí si pořizovat kartu novou. Anebo je možné kartu zálohovat finanční jistinou.

4.1.4 Jiné ochranné prvky

Ochranným prvkem na kartě je například fotografie uživatele. Fotografie se pořizuje při vyplňování žádosti o kartu. Dalším ochranným prvkem na kartě je například vytištěné nebo vyražené jméno uživatele. Na kartě bývá vytištěno nebo vyraženo také unikátní číslo karty uživatele. Mohou zde být použity také různé hologramy, speciální tiskové techniky – například klopný efekt, prvky viditelné pouze v dopadajícím ultrafialovém či jiném záření.

---

[30] ISO. *International Organitazation for Standardazation*, [online]. 2003

Čipová karta pro podporu turistického ruchu v regionu jednoznačně nemusí patřit jednomu uživateli nebo skupině uživatelů. Kartu může vlastnit cestovní kancelář, která bude mít předplaceno například 500 vstupů do určitého zařízení (samozřejmě s množstevní slevou). Přijede-li skrze cestovní kancelář do zařízení autobus turistů, odečte se z karty 50 vstupů.

4.2 Elektronické bezpečnostní prvky turistické karty

Elektronické bezpečnostní prvky je vhodné kombinovat s prvky neelektronickými (barva, fotografie apod). Pro městskou kartu s podporou turistického ruchu byly vybrány tyto elektronické bezpečnostní prvky:

- Jedinečné identifikační číslo – každá karta je identifikována svým ID číslem, které je celosvětově jedinečné a je pevně vypálené v paměti výrobcem karty. Toto číslo bývá využito v jednodušších aplikacích typu kontroly vstupu nebo identifikace, kde jsou data o nositeli karty uložena na serveru společně s číslem karty. U procesorových karet může být číslo karty jedno z bezpečnostních prvků při komunikaci s kartou – např. data zakódovaná pro jednu konkrétní kartu jiná karta odmítne.
- Šifrování komunikace – lepší karty svoji komunikaci se čtecím zařízením šifrují. Šifrování komunikace nabývá na významu u bezkontaktních karet, kde je riziko odposlechu vyšší.
- Šifrování přenášených dat – narozdíl od předchozí varianty se zde o šifrování stará aplikace, uložená na kartě. Většinou se používají symetrické šifry, které jsou rychlé a při vhodně zabezpečeném klíči i velmi bezpečné.[31]
- Limit pro platební operace - limit pro platební operace bezkontaktní kartou by měl být stanoven na určitou částku za den, například 500 Kč. Pokud uživatel překročí tuto částku, měla by obsluha u platebního terminálu vyžadovat PIN kód anebo jiný specifický kód, který je přiřazen uživateli při pořízování bezkontaktní čipové karty.

[31] HENDRY, M. *Smart Card Security and Applications.* Boston, 2001

Další možné elektronické bezpečnostní prvky, které jsou však nevhodné pro zmiňovanou turistickou čipovou kartu:

- Digitálně podepsaná data – data uložená na kartu mohou být podepsána digitálním podpisem. Pokud je součástí podepsaných dat i ID karty, jsou data veřejně čitelná, ale nelze je přenést na jinou kartu – na ní budou brána jako neplatná.
- Elektronický podpis a asymetrická šifra – mikroprocesorové karty mohou sloužit jako nositel digitálního certifikátu s privátním klíčem a sloužit k šifrování a podepisování, které probíhá na kartě. Protože běžnému karetnímu čipu by trvalo šifrování příliš dlouho (řádově sekundy i více), jsou karty, které mají sloužit k tomuto účelu, vybaveny kryptoprocesorem, urychlujícím výpočet až na desítky milisekund. [32]

4.3 Kombinace ochranných prvků

Kombinace ochranných prvků by měly sloužit pro větší bezpečnost používání karty. Kombinují se ochranné prvky neelektronické, jako jsou barva, vytlačené písmo, hologram apod. s prvky elektronickými. Příkladem může být situace, kdy dospělý jedinec využije pro vstup do určitého zařízení kartu určenou pro děti. Dospělý může být obsluhou odhalen, jak pro něj nesprávnou barvou karty, tak daty o uživateli nahranými na kartě.

Dalším příkladem kombinování ochranných prvků na kartě je kombinace čipu a čárového kódu. Jedná se tedy o kombinaci aktivních a pasivních prvků. Určitá data mohou být uložena v čipu karty a další údaje, jako je například identifikační číslo uživatele pro danou aplikaci, mohou být uloženy na čipu.

Vhodným ochraným prvkem je také nastavení ověřování platby nebo použití karty sms zprávou. Stejný systém funguje například u internetového bankovnictví.

---

[32] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi*, Olomouc, 2008

4.4 Možnosti zneužití čipové karty

Uživatel by měl při vyplňování zřizovacího formuláře souhlasit se zpracováním osobních údajů. Je snahou provozovatele aby minimalizoval možnosti zneužití, nicméně možností zneužití je celá řada. Prvním může být ztráta nebo odcizení karty. V takovém případě je možné kontaktovat kartové centrum a čipovou kartu nechat zablokovat. Dalším zneužítím karty může být naklonování, tedy okopírování nebo změna uložených údajů na kartě, což se u moderních systémů na bezpečnost ve většině případů jeví jako nemožné.

Zneužitím může být také situace, kdy uživatel kartu půjčí jiné osobě (druhá osoba ji může zneužít a ještě kartu například ani nevrátit majiteli). Proto je důležité mít na kartě jisté identifikační údaje, například fotografii nebo si nechat aktivovat funkci ověřování sms zprávou.

Zneužití však může být také interní, například obsluhou kartového centra. Obsluha kartového centra může zcizit data nebo celé datové balíky, týkající se uživatelů. Tato zcizená data pak dotyčný může prodat nebo je sám zneužít například pro marketingové účely.

4.5 Standardy bezpečnosti čipových karet

Podkapitola popisuje jednotlivé normy ISO, které se týkají zabezpečení čipových karet. Například norma ISO/IEC 7810 se zabývá identifikací karty, ve velké míře velikostmi karet. Jsou zde uvedeny jednotlivé formáty čipových karet a jejich využití. Norma ISO/IEC 7816 se zabývá spíše kontaktními kartami. Normy týkající se bezkontaktních karet jako ISO/IEC 10536, ISO/IEC 14443, ISO/IEC 15693 jsou popsány již v první kapitole, přesněji v podkapitole 1.5.

4.5.1 ISO/IEC 7810

ISO/IEC 7810 je standardizační norma pro identifikaci karty. Tento standard definuje fyzikální charakteristiky karet. Norma specifikuje požadavky pro takové fyzikální

vlastnosti, jako jsou: hořlavost, toxicita, odolnost proti chemikáliím, odolnost proti opotřebení při vystavování světlu a teplu, trvanlivost apod.

Norma také definuje velikosti karet. Dle zmíněné normy existují čtyři typy karet popsané v tabulce níže. Všechny karty mají tloušťku 0,76 mm.

Tabulka 4: Formáty karet

Formát	Rozměry	Použití
ID-1	85,60 × 53,98 mm	Většina bankovních karet a průkazy totožnosti
ID-2	105 × 74 mm	Německé průkazy vydané před listopadem 2009
ID-3	125 × 88 mm	Pasy a víza
ID-000	25 × 15 mm	SIM karty

Zdroj: Český normalizační institut

ID-1

Karta formátu ID-1 má rozměry 85,6 x 53,98 mm. Je běžně využívaná pro platební karty. V některých zemích se využívá také pro řidičské průkazy a průkazy totožnosti. Tento formát je také běžný pro věrnostní karty různých maloobchodů. V USA se v tomto formátu dělají cestovní pasy.

ID-2

Karta ve formátu ID-2 má rozměry 105 x 74 mm. Tento formát se využívá například pro víza. Formát byl do konce října roku 2009 používán v Německu jako formát pro občanské průkazy. Od listopadu roku 2009 budou občanské průkazy v Německu vydávány ve formátu ID-1.

ID-3

Karta ve formátu ID-3 má rozměry 125 x 88 mm a používá se po celém světě jako formát určený pro cestovní pasy.

ID-000

Formát ID-000 má rozměry 25 x 15 mm a má jeden roh nepatrně zkosen. Tento formát se využívá pro SIM karty.

4.5.1 ISO/IEC 7816

ISO/IEC 7816 je řada mezinárodních norem, které specifikují karty s integrovanými obvody a použití těchto karet pro mezinárodní výměnu. Tyto karty jsou identifikačními kartami určenými pro výměnu informací vyjednávaných mezi vnějším světem a integrovaným obvodem v kartě. Výsledkem výměny informací je informace dodaná kartou (výsledek výpočtu, uložená data) anebo modifikace obsahu karty (ukládání dat resp. zapamatování).

Pět částí je specifických pro karty s galvanickými kontakty a tři z nich specifikují elektrické rozhraní:

- ISO/IEC 7816-1 specifikuje fyzikální charakteristiky karet s kontakty.
- ISO/IEC 7816-2 specifikuje rozměry a umístění kontaktů.
    - ISO/IEC 7816-3 specifikuje elektrické rozhraní a protokoly přenosu pro asynchronní karty.
    - ISO/IEC 7816-10 specifikuje elektrické rozhraní a odpověď na reset pro synchronní karty.
    - ISO/IEC 7816-12 specifikuje elektrické rozhraní a pracovní procedury pro USB karty.

Všechny další části jsou nezávislé na technologii fyzického rozhraní. Platí pro karty, ke kterým je přistupováno pomocí kontaktů a/nebo radiofrekvenčně.

- ISO/IEC 7816-4 specifikuje organizaci, bezpečnost a příkazy pro výměnu.
- ISO/IEC 7816-5 specifikuje registraci poskytovatelů aplikací.

- ISO/IEC 7816-6 specifikuje mezioborové datové prvky pro výměnu.
- ISO/IEC 7816-7 specifikuje příkazy strukturovaného dotazovacího jazyka karty.
- ISO/IEC 7816-8 specifikuje příkazy pro bezpečnostní operace.
- ISO/IEC 7816-9 specifikuje příkazy pro správu karet.
- ISO/IEC 7816-11 specifikuje biometrické metody ověřování osob.
- ISO/IEC 7816-15 specifikuje aplikaci kryptografické informace.[33]

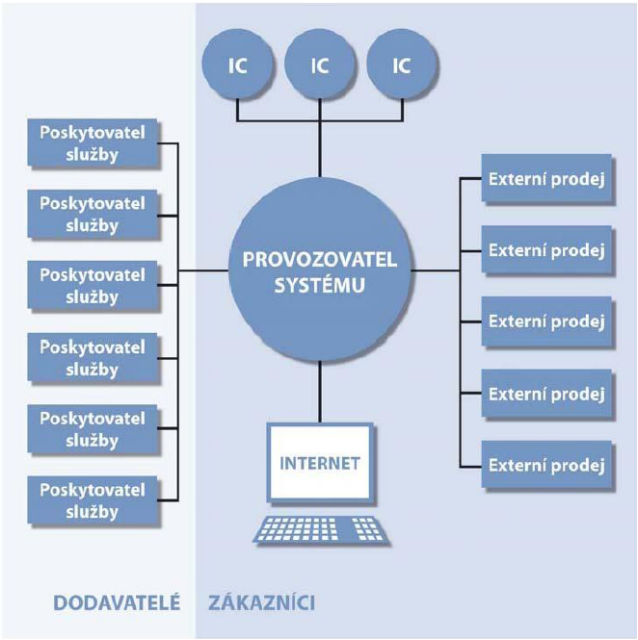
[33] Česká technická norma. *Identifikační karty - Karty s integrovanými obvody*, [online]. 2005

5. Návrh architekury systému a popis procesů

Pátá kapitola navrhuje celkovou architekturu systému pro zavedení turistické čipové karty, základní funkcionalitu systému, nástroje jednotlivých skupin uživatelů. Dále kapitola popisuje prodejní procesy turistické čipové karty, akceptaci karet, systém sběru dat. Kapitola se zmiňuje o nutnosti reportů a statistik. V kapitole je specifikován software potřebný pro fungování systému turistické čipové karty, struktura kódu čipové karty a komponenty systému – nároky na vybavení.

5.1 Celková architektura

Data systému jsou shromažďována v centrální databázi a následně jsou zpracována aplikací na centrálním serveru. Součástí systému jsou prodejní místa, akceptační místa, přičemž některá místa mohou být obojí. Tato místa generují vstupní data o prodejích karet a jejich využívání u jednotlivých poskytovatelů služeb v rámci systému. Jako prodejní centra fungují informační centra regionu a další subjekty (externí prodej). Poskytovatelé služeb zahrnutých do karty jsou akceptačními místy systému. Dalším internetovým kanálem mohou být internetové stránky systému turistických karet, umožňující přímý prodej produktu koncovému zákazníkovi.



Obrázek 11: Architektura systému

Zdroj: Studie technického řešení digitalizace Olomouc region Card

5.1.1 Základní funkcionalita systému

Systém turistické čipové karty musí být schopen evidovat subjekty zapojené do systému – prodejci, akceptanti, přímí zákazníci, přidělování práv těmto subjektům. Systém eviduje karty s možností generovat karty, nahlížet do historie karet a jejich vazeb na zapojené subjekty. Další funkcí je například trasování použití karet.

Systém spravuje tyto agendy:

- Agenda on-line prodeje a jeho plateb.
- Agenda pultového prodeje karet s možností generování stavu prodejů, automatizované logistiky zásobování prodejních míst.
- Agenda zpracování vyúčtování prodejů.
- Agenda reportů o stavu systému a statistikách.
- Agenda sestavování obsahů karet (typové balíčky služeb).
- Agenda komunikace se zapojenými subjekty včetně možnosti on-line hlášení změn, poruch, žádostí apod.
- Agenda importu off-line pořízených dat.
- Agenda zpracování refundací poskytovatelům služeb za užití karet v jejich zařízení.
- Správa webových stránek systému.[34]

5.1.2 Nástroje jednotlivých skupin uživatelů

Skupiny v systému turistických čipových karet byly určeny čtyři. Jsou to správce systému (správa systému může být rozdělena mezi více kompetentních osob se specifickými právy), prodejci (pultový prodej), akceptanti a koncoví zákazníci. V této podkapitole jsou popsány nástroje pro fungování systému těchto čtyř skupin.

Správce systému má na starosti:

[34] Regionální agentura pro rozvoj severní Moravy, *Studie technického řešení digitalizace Olomouc region Card*, Olomouc, 2009

- Zakládání, editaci a prohlížení evidenčních listů subjektů zapojených do systému.
- Dohled nad objednávkami, platbami, fakturací on-line objednávek.
- Sestavování balíčků pro jednotlivé typy karet.
- Dohled nad datovými toky údajů o prodejích a akceptacích s možností ručního zadání či importu off-line dat.
- Schvalování a korekce změn hlášených zapojenými subjekty.
- Vystavování a automatická distribuce vyúčtování refundací poskytovatelům služeb za smluvené období.
- Generování, export a tisk reportů o prodejích, akceptacích, trasování, souhrnných statistikách apod.
- Obsahová správa webové prezentace turistické čipové karty a případného e-shopu.

Akceptant:

- Validuje (ověření platnosti) karty pomocí čtečky nebo terminálu.
- Nahlíží do akceptačních statistik daného místa.
- Nahlašuje změny v akceptačním místě (například změny nabídky služeb, otvíracích hodin apod.).
- Má možnost trvalého přihlášení k centrální databázi (rozhraní musí být kdykoliv okamžitě k dispozici).

Prodejce (pultový prodej):

- Eviduje prodané karty (zápisem kódu na prázdnou kartu).
- Žádá další karty od distributora v případě, že klesne počet karet pod určitou hranici.
- Nahlíží do prodejních statistik daného místa.
- Má možnost trvalého přihlášení k centrální databázi (rozhraní musí být kdykoliv okamžitě k dispozici).

Koncový zákazník:

- Má možnost vyhledání prodejního místa.

- Má možnost prohlídky jednotlivých typů karet.
- Má možnost komunikovat se správcem systému.
- Využívá doplňkové platební služby.[35]

5.1.3 Prodejní procesy

Zákazník si může obstarat turistickou čipovou kartu dvěma způsoby – zakoupením na internetu nebo na místě (například v informačním centru). On-line prodej probíhá tak, že si zákazník vybere kartu, o kterou má zájem a vloží ji do košíku. Vybere si možnost platby – dobírkou, bankovním převodem, platební kartou, PaySec. Poté je karta fyzicky zaslána do místa bydliště zákazníka. Následně je v centrální databázi založen záznam prodané karty s vazbou na údaje o zákazníkovi a atributem o realizovaném prodeji. Zároveň je v agendě faktur vytvořen záznam o vystavené a e-mailem odeslané faktuře.

V případě, že si zákazník kupuje kartu na místě, rozhoduje se s podporou obsluhy, o kterou kartu má zájem. Po vybrání vhodné karty obsluha vloží prázdnou čipovou kartu do terminálu a pomocí prodejního rozhraní na ni nahraje kód vygenerovaný systémem. V případě čipové karty dojde v okamžiku příchozího požadavku o prodej k vygenerování příslušné karty podobně jako v případě on-line prodeje, jen s tím rozdílem, že se neevidují údaje o zákazníkovi. Záznam karty se rovnou označí atributem o prodeji. V případě pultového prodeje je zákazník anonymní.

5.1.4 Akceptace

Postup při akceptaci probíhá tak, že obsluha vloží kartu do čtečky nebo terminálu. Terminál odešle v případě on-line rozhraní kód přečtený z čipu do centrální databáze. Zde se ověří, zda daný kód již nebyl v daném zařízení využit, zda je služba daného zařízení obsažena v příslušném typu karty. V případě off-line validace se kód neodesílá, ověření proběhne přímo v terminálu. Je-li výsledek předešlého ověření pozitivní, terminál dále ověří, zda je v čipu karty již zaznamenán datum a čas prvního použití karty. Pokud je,

[35] ŠUFFNER, R. *Liberecká městská karta, funkční specifikace*, Liberec, 2006

ověří, zda probíhá aktuální akceptace ve lhůtě časové platnosti daného typu karty. Pokud není, zaznamená se do čipu aktuální datum a čas. Je-li validace časové platnosti pozitivní, oznámí terminál opravnění čerpání služby. V případě off-line terminálu se zaznamená použitý kód do paměti zařízení.

Akceptační rozhraní musí umožňovat akceptovat kartu pro více služeb na jedné pokladně. Například v zařízeních, které v rámci návštěvnické karty nabízejí více různých služeb (více prohlídkových okruhů na zámku apod.).

5.1.5 Sběr dat

Místa, která jsou on-line, odesílají veškerá data průběžně v reálném čase. Místa, která jsou off-line (případně jen dočasně), musí ve smluvené periodě odesílat zaznamenaná data do centrální databáze. Off-line terminály lze připojit přes USB rozhraní. Data je možné nahrát na flashdisk, nakopírovat do jiného počítače, který disponuje připojením k internetu a odeslat je prostřednictvím webového rozhraní nebo emailu přímo do centrálního systému.[36]

5.1.6 Reporty a statistiky

Reporty a statistiky lze nadefinovat více způsoby, dle potřeb – z hlediska analýzy provozu systému, obchodních a marketingových ukazatelů. Sledovány budou statistiky prodeje a statistiky akceptací.

Statistiky prodeje:

- Prodeje dle typů jednotlivých typů karet (dle délky platnosti, druhu – individuální, dětská apod).

[36] Regionální agentura pro rozvoj severní Moravy, *Studie technického řešení digitalizace Olomouc region Card*, Olomouc, 2009

- Vývoj prodeje v různých měsících.
- Statistiky prodeje dle distribučních kanálů (pultový prodej, internetový prodej).
- Žebříček úspěšnosti jednotlivých prodejců (objemy prodejů podle tržeb nebo podle počtu karet).

Statistiky akceptací:

- Žebříček akceptantů dle poskytovaných služeb.
- Žebříček nejvyužívanějších akceptací.
- Výpis stavu čerpání karet k určitému datu (kolik prodaných karet ještě nebylo aktivováno, kolik je ve fázi časové platnosti a kolik je expirovaných).
- Trasování karty (výpis historie použití konkrétní karty).[37]

5.1.7 Struktura dat evidenčního listu akceptačního místa

Evidenční list akceptačního místa je strukturovaný záznam v databázi, který soustřeďuje všechny informace o příslušném poskytovateli, službách zapojených do systému turistické karty. Tyto informace slouží jednak pro koncového zákazníka, dále pro prodejce, pro správce systému a pro systém samotný. Systém by měl být ideálně připraven i na jistý stupeň dynamického fungování v průběhu roku (měl by například umět automaticky aktualizovat na webové prezentaci otevírací doby zahrnutých zařízení dle aktuálního měsíce, v zimním období by měl automaticky zveřejňovat zimní fotografie zařízení apod.). Doporučená struktura zaznamenávaných dat o zahrnuté službě (akceptačním místě) je uvedena níže.

Tabulka 5: Konceptuální návrh struktury databáze evidenčního listu

ID zařízení
Název zařízení

[37] Kylar, S. *Karta hosta Jeseníky – studie proveditelnosti*, [online]. 2009

Uživatelské jméno provozovatele zařízení (vazba do adresáře zapojených subjektů)
Atribut „plátce DPH“
Atribut aktivnosti
Časové omezení aktivnosti (v provozu od-do)
Poskytovaná sleva držiteli karty v % (volný vstup bude 0%)
Výše refundace za užití karty typu A,B,C (například individuální, rodinná, dětská)
Vzdálenost od Liberce
Atraktivita (škála hvězdiček)
Nutnost rezervace služby předem (+ telefonní číslo pro rezervace)
Dopravní dostupnost
Popis služeb
Technické vybavení místa (on-line, off-line PC, off-line terminál, bez prostředků)
Sezonalita služeb (zima od-do, léto od-do, celý rok)
Provozní doba v období od-do (možnost zakládat více tabulek pro různá roční období)
Omezení provozu dle počasí
Jazyky, kterými komunikuje personál
Výluky provozu

Kategorie zařízení (sport, kultura, památka, relaxace, zdraví, ubytování, restaurace, rodina, zábava, poznávání apod.)
Letní foto/zimní foto, fotogalerie
www zařízení
Návštěvnost zařízení
GPS
Kontakty

Zdroj: Studie technického řešení digitalizace Olomouc region Card

5.1.8 Struktura dat evidenčního typu karty

Databáze obsahuje také číselníky typů karet. Jednotlivé typy karet se mohou lišit kombinací služeb zahrnutých na kartě. Mohou se lišit také cenou, délkou platnosti, podmínka užití (individuální, rodinná karta). Doporučená struktura dat o typu karty je uvedena níže.

Tabulka 6: Koncepce návrhu struktury dat evidenčního typu karty

ID karty
Název typu karty
Délka platnosti karty
Vyobrazení karty
Koncová cena karty

Zahrnutá zařízení poskytující služby
Popis karty
Druh karty (individuální, rodinná,…)
Systémem přidělená neunikátní část kódu karty (více v kapitole Struktura kódu)

Zdroj: Studie technického řešení digitalizace Olomouc region Card

5.2 Aplikační software

Při zavádění turistické čipové karty, je nutné vyvinout příslušný aplikační software, který bude mít na starosti čtyři základní aplikace – řídící aplikaci, on-line terminál, off-line terminál v PC, off-line mobilní terminál.

Řídící aplikace

Tato aplikace musí fungovat jako on-line systém přístupný běžným skupinám uživatelů přes webové rozhraní. Musí zajistit funkcionalitu celého systému. Aplikace využívá SQL databázi s veškerými bezpečnostními standardy. Systém musí jít kdykoli rozšířit nebo upravit v závislosti na měnících se požadavcích provozovatele. Řídící aplikace poskytuje funkcionalitu všem skupinám uživatelů přes specifická webová rozhraní. Součástí řídící aplikace je také redakční systém pro správu internetových stránek systému. Součástí stránek může být také e-shop pro přímý prodej turistických čipových karet (zásilkový prodej). Pro řídící aplikaci je vyžadován SSL certifikát a platební brána pro transakce platebními kartami a systém PaySec[38].

[38] Konto PaySec je systém pro rychlé a bezpečné nakupování na internetu. Pomocí předplaceného konta ("elektronické peněženky") je možné v reálném čase platit na online aukcích či za služby, obsah a zboží u obchodníků, kteří mají svůj systém napojený na PaySec.

On-line terminál

On-line terminál musí být přístupný přes webové rozhraní. Jeho funkce musí být jištěna řešením přechodu do off-line režimu s lokální validací kódu karty s ukládáním použitých kódů do souboru v daném počítači. Při validaci karty musí on-line terminál obsluze identifikovat zákazníka (pokud je karta zakoupena v e-shopu), identifikovat typ karty a zobrazit známou historii dosavadního užití karty.

Dále musí umožňovat volbu, zda se jedná o prodej karty nebo akceptaci karty. Pokud se jedná o akceptaci, musí umožňovat také volbu služby, která je čerpána (poskytuje-li akceptační místo více služeb). Tyto volby musí mít každé místo nakonfigurovány individuálně (dle toho, zda je to prodejní nebo akceptační místo nebo obojí a dle toho, jaké služby jsou zde dostupné). On-line terminál je takovým specifickým rozhraním řídící aplikace.

On-line terminál musí umožňovat přechod do záložního off-line režimu při výpadku připojení k internetu. V situaci, kdy nastane výpadek připojení k internetu je validita karty vyhodnocována off-line validátorem v lokálním PC a data o použití karty jsou ukládána do souboru v lokálním PC. Po obnovení připojení k intranetu je vyžadována možnost dávkového odeslání dat centrální databázi a vyčištění dočasných off-line úložišť.

Off-line terminál v PC

Off-line terminál je jednoduchá aplikace běžící lokálně na daném PC. Nejvhodnější je pro tuto aplikaci portable (přenosný) charakter bez nutnosti instalace a zápisu do registrů operačního systému. Podmínkou je maximální nezávislost na operačním systému (nutnost fungování na MS Windows 2000 a vyšších). Aplikace vyhodnotí, zda daná karta platí v příslušném zařízení, zda již nebyla v tomto zařízení použita a pokud je vše v pořádku, uložit informaci o jejím použití do paměti terminálu pro pozdější dávkové předání centrální databázi.

Podobně jako on-line terminál, umožňuje off-line terminál volbu, zda se jedná o prodej nebo akceptaci karty. Pokud se jedná o akceptaci, musí umožňovat také volbu služby, která je čerpána (poskytuje-li akceptační místo více služeb).

Off-line mobilní terminál

Off-line aplikace mobilního terminálu respektuje platformu a technické možnosti daného terminálu a dále maximální jednoduchost a přehlednost pro obsluhu. Součástí off-line aplikace mobilního terminálu musí být také SW pro rozhraní počítače zajišťující transfery dat mezi mobilním terminálem a centrální databází. Aplikace opět musí umět vyhodnotit, zda daná karta platí v příslušném zařízení, zda již nebyla použita. Informace o použití karty je uložena do paměti terminálu pro pozdější předání centrální databázi. Opět umožňuje volbu, zda se jedná o prodej karty nebo akceptaci karty.[39]

5.3 Struktura kódu

Kód by měl být tvořen dvěma částmi – identifikátorem karty a indetifikátorem zahrnutých služeb. Indentifikátor karty je 5-6 znakový unikátní kód. V případě internetového prodeje se na něj váže také záznam o zákazníkovi. Dle tohoto identifikátoru je možné zobrazovat tracking karty (historie jejího využití). Identifikátor karty slouží také při ověřování pokusu o opakované využití karty v určitém zařízení.

Druhá část kódu (až 15-16 znaků) identifikuje typ balíčku služeb zahrnutých v dané kartě. Z této části kódu lze vyčíst, jaká kombinace služeb je zahrnuta, jaká je časová platnost karty a o jaký druh karty z hlediska podmínek využití jde (rodinná, individuální,…). Tato část kódu už není unikátní, protože se váže na předdefinovaný typ. Tato struktura kódu zajistí možnost online i off-line validace platnosti karty včetně kontroly opakovaného použití karty.[40]

5.4 Komponenty systému – nároky na vybavení

Tato podkapitola popisuje nároky na vybavení subjektů zapojených do systému turistické karty. Pro centrální systém je nutné pořídit hardware sestávající z řídícího serveru, externího zálohovacího disku a záložního zdroje. Nároky na software jsou v podobě

[39] Kylar, S. *Karta hosta Jeseníky – studie proveditelnosti*, [online]. 2009

[40] RANKL, W. *Chipkarten-Anwendungen. Entwurfsmuster für Einsatz und Programmierung von Chipkarten*, München, 2006

operačního systému s podporou webserveru a řídících aplikací. Níže jsou zmíněné nároky popsány konkrétně.

Hardware centrálního systému sestává z:

- Řídícího serveru – webserver – spolehlivý značkový webserver s min. dvěma čtyřjádrovými procesory 1,86 GHz, 18 MB mezipaměti, 16 GB-R RAM, síťový adaptér 1GbE, dvěma porty, rychlým řadičem disků, rychlým systémovým serverovým diskem 300GB, rychlými serverovými datovými disky min. 3x500 GB (RAID) a SW pro správu včetně vzdálené správy. Záložní server případně jiné levnější záložní úložiště.
- Externího zálohovacího disku – základní periodické zálohování musí probíhat automaticky na zvláštní disk v základním serveru. Kromě toho musí být prováděny (například jednou měsíčně) ještě ruční zálohy na disk fyzicky umístěný mimo serverovnu. Externí disk 500 GB.
- Záložního zdroje – záložní zdroj UPS, min 1500 VA.

Provozní nároky na centrální systém obsahují:

- Servehousing – server musí být připojen k páteři internetu formou serverhousingu s konektivitou minimálně 100 Mb/s. Musí být garantován nepřetržitý dohled, technická podpora a možnost vzdálené správy.

Software centrálního systému sestává z:

- Operačního systému s podporou webserveru – webserver musí být vybaven operačním systémem a veškerými aplikacemi a knihovnami potřebnými pro porvoz řídící aplikace (v závislosti na řešení řídící aplikace). Předpokladá se provoz SQL databáze a PHP 5.

- Řídící aplikace – musí být takového analytického a funkčního rozsahu, aby splňovala veškeré požadavky uvedené v celé kapitole „Návrh architektury systému a popis procesů“. Předpokládá se on-line aplikace s webovými rozhraními pro jednotlivé skupiny uživatelů. Nutná je tedy také škálovatelnost oprávnění jednotlivých skupin. Její součástí musí být také redakční systém pro správu webové prezentace systému včetně SEO optimalizace prezentace a e-shopem pro prodej turistických karet formou zásilkového obchodu. Možnost snadné správy jazykových verzí web prezentace. Nutný bezpečnostní certifikát a platební brána pro platební karty a systémem PaySec.

Komponenty systému pro prodejní a akceptační místa, ve kterých mají PC s přípojením k internetu:

- On-line terminál čipových karet
- Ovládací software on-line terminálu komunikující s řídící aplikací v reálném čase s aplikací pro záložní validaci a sběr dat v době výpadku připojení k internetu. Po obnovení připojení musí SW umožňovat dávkové odeslání nasbíraných dat do centrální databáze.

Komponenty systému pouze pro akceptační místa, ve kterých mají PC bez připojení k internetu:

- On-line terminál čipových karet.
- Flashdisc 500 MB.
- Ovládací software on-line terminálu fungující v off-line režimu s aplikací pro validaci a sběr dat bez nutnosti spojení s centrální databází. Musí umožňovat dávkové vykopírování sebraných dat pro možnost transportu do centrální databáze.

Komponenty systému pouze pro akceptační místa, které nemají žádné vybavení, mají však elektrickou přípojku (stejné komponenty systému jsou také na místech, která nemají ani elektrickou přípojku):

- Off-line mobilní terminál čipových karet s možností zadání jakou službu zákazník využívá (pro akceptační místa s více zahrnutými službami).

- Validační aplikace off-line mobilního terminálu + program pro vykopírování dat z off-line mobilního terminálu.

Komponenty systému pro správce systému:

- On-line terminál čipových karet pro operace s čipovými kartami.
- Servisní notebook pro zásahy v terénu, nouzový sběr dat apod.
- Ovládací SW on-line terminálu a SW na propojení s centrální databází.[41]

5.4.1 Požadavky na čtečky čipových karet/terminály

V případě on-line čtečky kontaktních čipových karet postačí jednoduché stolní čtečky bez klávesnice (nepožaduje se zadávání PINu). Off-line terminál by měl být v podobě zařízení na bázi průmyslového PDA. Jsou k dispozici také modely, ketré umí číst jak čárový kód, tak kontaktní čipové karty. Operační systém může být například Windows Mobile.

U on-line čtečky čipových karet je vyžadováno připojení přes USB, kompatibilita s průmyslovými standardy, délka kabelu alespoň 1,8 metru a čtečka nesmí vyžadovat instalaci ovladače.

Off-line mobilní terminál čipové karty vyžaduje napájení dobíjecími akumulátory s dlouhou výdrží (minimálně 48 hodin provozu), možnost snadného dobíjení (nabíječka je součástí dodávky). Terminál musí bý schopen indikovat validitu karty vizuálně na displeji a také zvukově. Na displeji se musí zobrazovat stav akumulátoru, podobně jako na mobilním telefonu. Terminál by měl být odolný vůči vodě, prachu a také proti pádu z výšky. Terminál umoňuje snadné vykopírování uložených dat pomocí USB rozhraní. Rozmezí provozních teplot by se mělo pohybovat okolo -10 až +50°C. Posledním

[41] Regionální agentura pro rozvoj severní Moravy, *Studie technického řešení digitalizace Olomouc region Card*, Olomouc, 2009

požadavkem na terminál je klávesnice, která umožní obsluze zadat, jaká služba se z karty čerpá.[42]

5.5 Kartové centrum

Kartové centrum je řídícím prvkem celého systému. Kartové centrum bude spojeno s provozovatelem systému turistických karet, na kterého jsou napojeni ostatní externí prodejci, informační centra a poskytovatelé služeb (viz. obr.č. 12 – Architekrura systému). Procesy vykonávané Kartovým centrem jsou podrobněji popsány v kapitole 5.1 „Celková architektura".

Kartové centrum provádí správu životního cyklu karet - vydávání karet (distribuce do ostatních prodejních míst + e-shop), rušení karet (prostřednictvím on-line systému), ukončení platnosti karet. Kartové centrum zajišťuje personalizaci karet, to znamená nahrání požadovaných aplikací, spravuje čipové aplikace, nastavuje poplatky za kartu, provádí registrace (návštěvníkovi, kteří si objednají kartu online).

Kartové centrum spravuje veškeré informace o zákaznících, čipových kartách, provedených transakcích. Centrum umožňuje import nebo export dat z/do externích systémů (prodejní, akceptační místa) dle jejich požadavků (samozřejmě v omezené míře).

Centrum může mít na starosti centrální systém turistické karty, coby specifikum městské karty popsaný výše, tzn. zajišťování serverů, zálohovaní disků, softwaru a řídících aplikací. Levnější a praktičtější variantou by však bylo si tyto služby nechat outsourcovat externí firmou. Provozovatel si tedy může vybrat, jestli bude provozovat centrální systém zcela sám anebo si pro tyto účely najme externí firmu.

[42] Kylar, S. *Karta hosta Jeseníky – studie proveditelnosti*, [online]. 2009

6. Zhodnocení východisek používání čipových karet v městských aglomeracích

Turistická čipová karta nabízí možnost propojení stávajícího odbavovacího systému se slevovými systémy a elektronickou peněženkou. Každý obchodní systém zajišťuje toky dat a jejich zpracování způsobem podřízeným svému účelu. Otázky kompatibility systémů lze v obecné rovině posuzovat zejména dle způsobu ukládání zpracovaných dat, především z hlediska jejich formátů, využívání číselníků a jejich harmonizace. Dále lze kompatibilitu posuzovat podle struktury ukládaných dat, respektive míry krytí shodné struktury dvou či více systémů. Posuzují se také standardy koncových zařízení, formáty použitých kódů a bezpečnostní standardy, které zpravidla určují míru otevřenosti daného systému.

Dále je třeba specifikovat, co se čeká od propojení stávajících systémů. Zda je to omezení vícenásobného pořizování dat, automatizace některých procesů zpracování apod. Pokud plní systémy naprosto rozdílné funkce, pak lze většinou jejich propojení omezit pouze na vzájemnou výměnu zpracovávaných dat. To je případ systému turistické karty a například odbavovacího systému.

Informace na turistické kartě systému turistické karty říká, že držitel karty má například nárok na volný vstup do určitého druhu zařízení. Pro odbavovací systém daného zařízení je však tato informace nečitelná, protože využívá úplně jiného formátu používaných kódů. Čipové karty toto propojení umožňují. Pro návštěvníka to představuje výhodu mít jednu čipovou kartu plnící roli jak karty turistické, tak přístupové do vybraného zařízení. Nutnou součástí funkčnosti celého systému je jeho rozšíření například formou infocenter, kde budou nabíjecí stanice čipových karet či přímým propojením se systémem platebních karet.

6.1 Shrnutí vlastností technologií dle typu média

Pro zhodnocení je níže uvedena tabulka s vlastnostmi různých technologií. V první části diplomové práce jsou uvedeny služby, které jsou vyžadovány po turistické kartě. Je zde porovnání opět třech technologií – čárového kódu, čipu a technologie NFC.

Tabulka 7: Shrnutí vlastností technologií dle typu média

	Čárový kód	Čip	NFC, mobilní technologie
Možnost zavedení různých karet s odlišnou kombinací zahrnutých služeb, různou délkou platnosti a různými podmínkami užití	Ano	Ano	Ano
Unikátnost a tedy jednoznačná identifikovatelnost karty	Ano	Ano	Ano
Možnost on-line objednání služby (ne zaslání karty)	Ano	Ne	Ano
Možnost off-line provozu akceptačního místa	Ano	Ano	Omezeně (za využití SMS kódu)
Možnost off-line provozu prodejního místa	Ano	Ne	Omezeně (za využití SMS kódu)
Možnost validace bez technických prostředků	Ano	Ne	Omezeně (za využití SMS kódu)
Nároky na obsluhu koncových zařízení	Nízká kvalifikace personálu	Nízká kvalifikace personálu	Nízká kvalifikace personálu
Nároky na správu a údržbu	Nízká kvalifikace personálu	Nízká kvalifikace personálu	Nízká kvalifikace personálu
Řádové výrobní náklady karty	2,00 Kč	10 - 25,00 Kč dle typu, množství, bez slev	0 Kč, integrováno přímo v mobilu nebo na SIM kartě

Řádové náklady na vybavení on-line akceptačního místa (HW)	cca 1200,00 Kč	cca 1200,00 Kč	Platební terminál poskytován karetní společností na stejném principu jako terminál pro kreditní karty
Řádové náklady na vybavení off-line akceptačního místa	cca 17 000,00 Kč	cca 20 000,00 – 25 000,00 Kč	0 Kč při použití SMS kódů
Možnost plně automatizované kontroly časové platnosti karty	Ne	Ano	Ano
Nároky na softwarovou podporu	Střední	Střední	Střední
Možnost plně automatizovaného on-line prodeje	Ano	Ne	Ano
Možnost využití většího množství služeb na jednu kartu, opakované využití	Ne	Ano	Ano
Omezení pro sběr a zpracování dat (evidenční a statistické)	Žádné	Žádné	Žádné

Zdroj: Studie technického řešení digitalizace Olomouc region Card

Z tabulky vyplývá, že nejvhodnější technologií pro turistickou čipovou kartu by byla technologie NFC. Bohužel v dnešní době nemají všichni potenciální návštěvníci regionu mobilní telefon s touto technologií. Z tabulky je patrné, že čárový kód je ekonomičtější variantou. Jednu základní vlastnost však čárový kód nemá a to je pro tuto práci klíčová funkce – možnost využití většího počtu služeb na jednu kartu, opakované využití. Čipová karta je v současné době méně výhodnou variantou, ale díky sílícímu používání lze předpokládat stálé zlevňování karet. Splňuje však základní a již zmiňovanou vlastnost a to,

že je možné ji použít opakovaně a k většímu počtu služeb. Proto je vhodné zvolit čipovou kartu jako médium pro systém turistické karty.

6.2 Rozpočet

Tabulka níže nastiňuje rozpočet zavedení turistické karty regionu. Rozpočet však není kompletní. Tabulka uvádí pouze software a hardware. Do rozpočtu by měla být zařazena ještě projektová příprava, proces implementace a zaškolení v systému, vytvoření dokumentace (manuály), náklady související s případným e-shopem, propagace a reklama a v neposlední řadě hrubé roční provozní náklady. Ceny jsou uvedeny bez 20% DPH.

Tabulka 8: Rozpočet

Software	Kč/ks	Ks	Kč
Řídící systém včetně redakčního systému webové prezentace			cca 900 000
Web			cca 50 000
On-line terminál pro PC			cca 20 000
Off-line terminál pro PC			cca 20 000
Off-line mobilní terminál			cca 30 000
Komunikační SW pro stahování dat do off-line mobilního			cca 5 000

terminálu			
Hardware	Kč/ks	Ks	Kč
Centrální server	cca 190 000	1	cca 190 000
Záložní zdroj UPS	cca 20 000	1	cca 20 000
Notebook pro správce systému	cca 12 000	1	cca 12 000
On-line čtečka	cca 1 200	Záleží na počtu akceptačních míst, jejichž počet se bude každým rokem měnit	1200 x n
Off-line mobilní čtečka	cca 30 000	Záleží na počtu akceptačních míst, jejichž počet se bude každým rokem měnit	30 000 x n

Zdroj: Studie technického řešení digitalizace Olomouc region Card

Tabulka rozpočtu byla tvořena dle předlohy „Studie technického řešení digitalizace Olomouc region Card“. Ceny však byly porovnány na portále heureka.cz a upraveny dle aktuálních nabídek zboží. Cena webových stránek se pohybuje, dle nabídky malých firem podnikajících v oblasti internetových stránek, od 50-ti tisíc Kč. Záleží na míře požadavků od zadavatele. Cena záložního zdroje UPS se pohybuje okolo 20-ti tisíc Kč (při požadavku minimální kapacity 1500 VA).

6.3 Časový harmonogram

Průběh realizace projektu závisí na dosavadních zkušenostech, kapacitách a velikosti dodavatelské firmy. Harmonogram uvedený níže, vzhledem k rozsahu systému, počítá spíše s pomalejším průběhem. Projekt by bylo možné urychlit nasazením více terénních

techniků pro proces proškolování prodejních a akceptačních míst. Pro zkrácení doby zavedení projektu by bylo vhodné pořádat hromadná školení. Pro porovnání časové náročnosti jednotlivých fází realizace projektu je v tabulce uvedena také technologie čárového kódu.

Tabulka 9: Časový harmonogram

	Čárový kód (počet týdnů)	Čip (počet týdnů)
Projektová příprava	2	3
Příprava a úpravy SW	11	15
Implementace systému	2	3
Testování systému	1	2
Instalace a proškolování prodejních a akceptačních míst	7	9
Zkušební provoz	5	5
Ostrý provoz	1	1
Celková časová náročnost	29	38

Zdroj: Studie technického řešení digitalizace Olomouc region Card

Z tabulky je patrné, že využití technologie čárového kódu pro turistickou kartu je v samotném zavedení výrazně kratší než v případě technologie čipové karty. Čárový kód však nedokáže pokrýt požadavky na turistickou kartu jako je například elektronická peněženka. Pro tuto tabulku byl vzorem časový harmonogram realizace turistické čipové karty v olomouckém regionu. Vzhledem k velice podobnému počtu obyvatel Olomouce

a Liberce byly ponechány totožné časové údaje. Předpokladem je, že počet prodejních a akceptačních míst je v těchto dvou městech velmi podobný.

6.4 Výhled do budoucnosti

Vzhledem ke skutečnosti, že pro oblast ticketingových a odbavovacích systémů není předepsán žádný jednotný standard, může docházet k roztříštěnosti systému, jehož propojení by bylo klasickou HW cestou náročné. Využití SW mobilních aplikací skrývá potenciál v zastřešení služeb a využívání společných databází. Rozvojové aktivity bank a telefonních operátorů skýtají potenciál v masivním rozšíření NFC mobilních technologií, které budou využitelné a lehce aplikovatelné na slevové a návštěvnické systémy. [43]

U technologií NFC není třeba nic tisknout nebo objednávat. Na základě platební peněženky v telefonu je možné provést úhradu za službu a například dostat patřičnou slevu. Limit pro platební operace bývá většinou 500 Kč, přesáhne-li návštěvník tento limit, vyzve ho aplikace k zadání kódu na mobilním telefonu, jehož pomocí platbu autorizuje. Tento kód je uložen v zabezpečeném prostoru SIM karty mobilního telefonu a nahrazuje v tomto případě klasický PIN kód, který zadává klient u transakcí běžnou platební kartou.

V Evropě probíhá několik pilotních projektů zaměřených na NFC technologie, aliance NFC sdružuje více než 140 celoevropských firem a podniků. Automobilka BMW integruje do svých klíčů od vozů NFC čip, který dokáže otevřít dveře pokoje (při on-line rezervaci není nutné procházet recepcí a klient udělá veškeré transakce doma u počítače). V České republice přechází na technologii NFC první supermarkety (Globus), banky (Komerční banka, CITIBank) a mobilní operátoři (Telefonica, T-Mobile). Technologie čipů a mobilních telefonů je tedy výhodná pro přímé platební operace, které umí poskytovat definované slevy.[44]

---

[43] Regionální agentura pro rozvoj severní Moravy, *Studie technického řešení digitalizace Olomouc region Card*, Olomouc, 2009

[44] KOTLÁN, R. *CardMag Magazín: Bezkontaktní technologie*, [online]. 2009

7. Závěr

Diplomová práce se zabývá zavedením turistické varianty městské karty v regionu, která se snaží sjednotit již existující systémy Libereckého kraje. Diplomová práce má ambice být jedním z významných podkladů pro vypracování studie proveditelnosti, jež by vedla k zavedení těchto karet v regionu Statutárního města Liberec. Je určena zejména návštěvníkům regionu, které osloví početnými výhodami, jako jsou levnější vstupy do různých zařízení, elektronická peněženka apod. Každý investor takového projektu (obzvláště ten, který hospodaří s obecními prostředky) by si měl uvědomit, že tvorba oddělených systémů je z hlediska investice neefektivní a s ohledem na omezené zdroje je nutné hledat nejvhodnější alternativu. V tomto případě je touto nejvhodnější alternativou technologie čipu, konkrétně byla zvolena bezkontaktní čipová karta MIFARE DESfire, která se svými vlastnostmi nejlépe hodí pro plnění funkcí turistické čipové karty, jak vyplývá z analýzy provedené v kapitole popisující výběr vhodné technologie.

Důvodem, proč je technologie čárové kódu nevhodná, je skutečnost, že slevové systémy jsou při použití čárového kódu odděleny od přímých platebních systémů. Uživatel tedy nemůže použít čárový kód pro další platby, a tudíž je jeho provoz omezen. Z hlediska využití čipových karet je možnost využití vyšší i z důvodu, že je možné provádět platební operace do určitého finančního objemu. Platební technologie na bázi čipových karet umožňují při platbě zohlednit slevu a plní proto stejnou primární funkci jako čárové kódy, kterou rozšiřují o platební využití.

Stejné funkce jako čipová karta vykonává technologie NFC, která je nenáročná na nákup vybavení (je integrované v řadě chytrých telefonů, v SIM kartách). Jedná se o technologii, kdy poskytovatel karet MasterCard zavádí nové platební karty nahratelné do mobilního telefonu spolu s distribucí nových platebních terminálů, které se od stávajících terminálů liší o doplněk NFC služby.

Tato technologie má veliký potenciál a region by měl zvážit investici do staršího typu technologie, kterou bude muset z důvodu masivního rozšíření jiné technologie v horizontu několika let nahradit. Záleží tedy, v jakém časovém horizontu by region plánoval turistickou kartu zavést. Pokud za pět let, technologie NFC by byla nejspíše vhodnější volbou. Pokud by region chtěl uvést turistickou kartu do provozu již tento rok, bude

vhodnější zvolit technologii čipu. Přece jen v dnešní době nemá každý možnost vlastnit chytrý mobilní telefon se zabudovanou technologií NFC, ale během pěti let může být tato technologie významným konkurentem technochnologie čipu.

Diplomová práce se zaměřuje spíše na technickou a procesní stránku zavádění turistické karty. Velice důležité je však neopomenout marketing a propagaci celého projektu. Marketing a budování vztahů s veřejností je nedílnou součástí produktu a jeho dalšího rozvoje. V rámci stanovení standardního marketingového mixu je nutné nalézt soubor taktických marketingových nástrojů pro prvotní stanovení produktové, cenové, distribuční a komunikační politiky.

Splnění hlavního cíle práce došlo na základě provedení dílčích cílů v jednotlivých kapitolách práce, které popisují technologické možnosti identifikace, legislativy, ochranu osobních údajů uživatelů a modely implementace pro ucelený návh řešení jako komplexně funkčního celku. Zavedení by vyžadovalo provedení finanční analýzy ve vazbě na marketingový průzkum oblasti, na jejichž základě by bylo možné doporučit postup technického doporučení parametrů a nastavení postupů pro implementaci.

Seznam použité literatury

[1] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi,* 1. vyd. Olomouc: ANAG, 2008, 157 s. ISBN 978-80-7263-465-1

[2] BUDIŠ, P.; ŠTĚDROŇ, B. *Elektronické komunikace*, 1.vyd. Bratislava: Magnet Press Slovakia, 2008, 110 s. ISBN 978-80-89169-11-5

[3] JUŘÍK, P. *Svět platebních a identifikačních karet*, 2.vyd. Praha: Grada, 2001, 175 s. ISBN 80-247-0195-2

[4] RAK, R. *Biometrie a identita člověka ve forenzních a komerčních aplikacích,* 1.vyd. Praha: Grada, 2008. 631 s. ISBN 978-80-247-2365-5

Odkaz na monografie vydané v angličtině:

[5] DONOVAN, J. *Portable Electronics: World Class Designs.* 1st ed., Burlington: Elsevier Inc. 2009. 554 pgs. ISBN 978-1-85617-624-8

[6] FINKENZELLER, K. *RFID Handbook.* 2nd ed., Chichester: John Wiley & Sons, Ltd., 2003. 427 pgs. ISBN 0-470-84402-7

[7] HENDRY, M. *Smart Card Security and Applications.* 1st ed., Boston: Artech House Publishers, 2001. 285 pgs. ISBN 1-58053-156-3

[8] MARKANTONAKIS, K.; MAYES K. *Smart Cards, Tokens, Security and Applications.* 1st ed., London: Springer Science + business Media, LLC. 2008, 392 pgs. ISBN-13: 978-0-387-72197-2

Odkaz na monografie vydané v němčině:

[9] EFFING, W.; RANKL, W. *Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards,* 5. Aus. München: Carl Hanser Verlag, 2008. 1088 Seiten. ISBN 987-3-446-40402-1

[10] RANKL, W. *Chipkarten-Anwendungen. Entwurfsmuster für Einsatz und Programmierung von Chipkarten*, 1.Aus. München: Carl Hanser Verlag, 2006. 206 Seiten. ISBN 3-446-40403-1

Odkaz na internetové zdroje:

[11] CardWerk. *Java Card Technology, Multos* [online]. 2009, [cit. 2009-03-27]. Dostupný z WWW: http://www.cardwerk.com

[12] Česká technická norma. *Identifikační karty - Karty s integrovanými obvody*, [online]. 2005, [cit. 2009-04-11]. Dostupný z WWW: http://nahledy.normy.biz/nahled.php?i=72443

[13] European Court of Human Rights. *Úmluva o ochraně lidských práv a základních svobod.* [online]. 2009, [cit. 2009-03-29]. Dostupný z WWW: http://www.echr.coe.int/NR/rdonlyres/82E3CE7F-5D3D-46EB-8C13-4F3262F9E20B/0/CZE_CONV.pdf

[14] GlobalPlatform. *Card Specifications*, [online]. 2009, [cit. 2009-03-27]. Dostupný z WWW: http://www.globalplatform.org

[15] ISO. *Interantional Organization for Standardization*, [online]. 2003, [cit. 2009-04-20]. Dostupný z WWW: http://www.iso.org/iso/catalogue_detail?csnumber=31432

[16] KOTLÁN, R. *CardMag Magazín: Bezkontaktní technologie*, [online]. 2009, [cit. 2009-04-05]. Dostupný z WWW: http://cardmag.cardzone.cz/archiv/cm2.pdf

[17] KYLAR, S. *Karta hosta Jeseníky – studie proveditelnosti*, [online]. 2009, [cit. 2009-04-03]. Dostupný z WWW: http://www.kr-olomoucky.cz/clanky/dokumenty/2499/fin-karta-hosta-jeseniky-sp-v6.pdf

[18] LipnoCard. *Všeobecné smluvní podmínky*, [online]. 2009, [cit. 2009-03-29]. Dostupný z WWW: http://www.lipnocard.cz/smluvni-podminky/

[19] Mikroelektronika. *Odbavovací systémy.* [online]. 2009, [cit. 2009-03-27]. Dostupný z WWW: http://www.mikroelektronika.cz/odbavovaci-systemy/text/produkty/automaty-na-vydej-jizdenek

[20] Ministerstvo dopravy České republiky. *Legislativa - silniční doprava - §5 vyhlášky MD č. 175/2000 Sb.*, [online]. 2006, [cit. 2009-03-28]. Dostupný z WWW: http://www.mdcr.cz/cs/Legislativa/Legislativa/Legislativa_CR_silnicni/silnicni-doprava.htm

[21] Ministerstvo dopravy České republiky. *Legislativa - silniční doprava*, [online]. 2006, [cit. 2009-03-29]. Dostupný z WWW: http://www.mdcr.cz/cs/Legislativa/Legislativa/Legislativa_CR_silnicni/

[22] NXP, *Mifare Type Identification Procedure.* [online]. 2009, [cit. 2009-03-28]. Dostupný z WWW: http://www.nxp.com/documents/application_note/AN10833.pdf

[23] Palán, M. *Bezkontaktní čipové karty Českých drah.* Vědeckotechnický sborník ČD č.21/2006. [online]. 2006, [cit. 2009-03-28]. Dostupný z WWW: http://www.cdrail.cz/vts/CLANKY/vts21/2108.pdf

[24] PANDATRON – Elektrotechnický magazín. *Karty s magnetickým pruhem.* [online]. 2008, [cit. 2009-03-26]. Dostupný z WWW: <http://pandatron.cz/?535&karty_s_magnetickym_pruhem>

[25] Registry.cz. *Legislativní aspekty: Evropská unie.* [online]. 2009, [cit. 2009-03-29]. Dostupný z WWW: http://www.registry.cz/index.php?pg=legislativni-aspekty--evropska-unie

[26] Úřad pro ochranu osobních údajů. *Zákon pro ochranu osobních údajů.* [online]. 2009, [cit. 2009-03-29]. Dostupný z WWW: http://www.uoou.cz/uoou.aspx?menu=4&submenu=5&loc=20

Jiné:

[27] POPELKA, P.; VIMR, M. *Systém městské čipové karty pro město Plzeň*, 2003

[28] Regionální agentura pro rozvoj severní Moravy, *Studie technického řešení digitalizace Olomouc region Card*, Olomouc, 2009

[29] ŠUFFNER, R. *Liberecká městská karta, funkční specifikace*, Liberec, 2006